

Erkki Saarikoski

**TIEDUSTELULAIT MUUTTUVASSA HYBRIDIUHKIEN
MAAILMASSA**



JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Saarikoski, Erkki

Tiedustelulait muuttuvassa hybridiuhkien maailmassa

Jyväskylä: Jyväskylän yliopisto, 2022, 97 s.

Kyberturvallisuus, pro gradu -tutkielma

Ohjaaja: Kari, Martti

Tämän tutkimuksen tarkoituksena on vastata kysymykseen, kuinka viranomaiset voivat tiedustelulakien mukaisilla toimivaltuuksilla torjua niitä kansallisen turvallisuuden uhkia, joita hybridiuvaikuttamisen keinoin on mahdollista synnyttää. Jotta kysymykseen voidaan vastata, tutkimuksessa määritellään valitun tutkimusaineiston perusteella kansallinen uhkakuvakäsite, josta johdetaan kansallinen hybridiuhkakäsite. Tähän käsitemuodostukseen käytetään ankkuroitua menetelmää.

Tutkielmassa kerrotaan myös suomalaiset tiedustelulait sekä toimivaltaiset tiedusteluviranomaiset. Tiedustelulakien osalta tutkielmassa tehdään kansainvälistä vertailua siitä, kuinka eräissä muissa Euroopan valtioissa tiedustelutoimivaltuudet ovat toteutettu. Tutkimusaineisto koostuu Suomen valtion virallisista asiakirjoista, kuten hallitusohjelmasta ja hallinnonalakohtaisista selonteista sekä poikkihallinnollisista turvallisuusasiakirjoista.

Tutkimusprosessin tuloksena syntyy vastaus, että nykymuotoisilla tiedustelulaeilla voidaan vastata niihin hybridiuhkiin, joita kansallisesti käsitämme tällä hetkellä hybridiuhkiin kuuluvaksi. Myös huomataan, että kybervaikuttaminen näyttölee varsin suurta roolia valtiollisissa teksteissä, kun tarkastellaan hybridiuhkien mukaisia uhkatekijöitä. Osassa lähdemateriaalia viranomaiset toteavat myös sen, että hybridiuhkien kenttään kuuluvat myös sellaiset vaikutusmekanismit, joita ei välttämättä nykyhetkessä kyetä tunnistamaan tai kategorisoimaan osaksi hybridiuhkia.

Samantyyppistä hybridiuhkia ja tiedustelulakien toimivaltuuksia toisiinsa vertailevaa tutkimusta ei ole aiemmin tehty, joten suoranaisesti tämän tutkimuksen tulokset eivät voi vahvistaa tai kumota mitään edellisiä tuloksia. Pikemminkin tämän tutkimuksen tulokset muodostavat pohjan jatkokeskustelulle ja -tutkimukselle. Jatkotutkimustarpeiksi tunnistetaan muun muassa se, että hybridiuhkien muuttuvan luonteen takia mielekäästä voisi olla seuranta, kuinka valtiollisissa narratiivissa hybridiuhkakäsitteen eri uhkatekijöiden painoarvot muuttuvat.

Asiasanat: tiedustelulait, hybridiuhka, hybridiuvaikuttaminen, informaatiovaikuttaminen.

ABSTRACT

Saarikoski, Erkki

Intelligence Laws in a Changing World of Hybrid Threats

Jyväskylä: University of Jyväskylä, 2022, 97 p.

Cyber Security, Master's Thesis

Supervisor: Kari, Martti

The purpose of this research is to answer the question on how state authorities can, with the mandates given by intelligence laws, prevent those risks to national security that are caused by hybrid threats. To be able to answer this question, during the research process concept of 'national threat image' is defined by using specific research material. And this national threat image is then evolved into national image of hybrid threats. This research and formation of national threats concepts is done by using grounded theory (GT) method.

Also, intelligence laws and regarding intelligence officials will be defined in Finnish context. Universal comparison about intelligence laws is done as well, when there are presented some case examples on how jurisdictional intelligence mandates are given to authorities in different countries in Europe. The research material constitutes from official documents of the Government of Finland, such as the Government Programme, government reports and cross-administrative security strategies.

As a result of research process is the finding, that current intelligence laws in Finland are valid when responding to those threats, that we nationally include under the concept of hybrid threats. Also is noted that cyber hostilities and affecting through cyber dimension plays significant role in those governmental documents which defines and describes the threats within the concept of hybrid threats. In few source materials governmental officials mentions that hybrid threats also include those kinds of ways of affecting which we currently cannot recognize at all or cannot categorize as a hybrid threat.

Similar comparative research between hybrid threats and intelligence law mandates has not been done in Finland before, so results of this this research does not directly confirm or repeal any previous research results. Instead, this research can serve as a basis for further studies. The recognized need for further studies rose from topics such as doing follow-up research on how hybrid threat concept is evolving in the governmental narrative.

Keywords: intelligence laws, hybrid threats, hybrid operations, information operations, influencing through information.

KUVIOT

KUVIO 1. Hybridivaikuttamisen käsite. (Suojelupoliisi, 2020)	35
KUVIO 2. Uhkakategoriat yksilöstä globaaliin.	45
KUVIO 3. Hybridiuhkien käsitekartta.....	52
KUVIO 4. Hybridiuhkakäsite vertailtuna tiedustelulakeihin.	62
KUVIO 5. Tallennuskapasiteetti. (Hilbert, 2015).....	65
KUVIO 6. Internetkäyttäjät (*: ennuste). (ITU, 2019).....	66

SISÄLLYS

TIIVISTELMÄ	2
ABSTRACT	3
KUVIOT	4
SISÄLLYS.....	5
1 JOHDANTO.....	7
1.1 Nykypäivän ilmiöitä hybridivaikuttamisesta	8
1.2 Aiempi tutkimus	9
1.3 Tutkielman tavoite, tutkimuskysymykset ja -rajaukset	11
2 TIEDUSTELUN ROOLI KANSALLISEN TURVALLISUUDEN TEKIJÄNÄ14	
2.1 Tiedusteluviranomaiset Suomessa.....	15
2.2 Tiedustelulait – mitä ne ovat ja mitä ne toivat?.....	18
2.2.1 Tiedustelulakien syntyminen	18
2.2.2 Tiedustelulakien tuomat toimivaltuusmuutokset.....	22
2.3 Tiedustelutoiminnan sääntely muissa maissa – tapausesimerkkejä ..	28
2.4 Turvallisuuskäsitteen suhde kansallisiin uhkakuviiin.....	32
2.5 Turvallisuusviranomaisten määritelmät hybridiuhkista.....	34
3 TUTKIMUSAINEISTO JA -MENETELMÄ, AINEISTON KOODAUS	37
3.1 Tutkimusaineisto	37
3.2 Tutkimusmenetelmä	40
3.3 Hybridiuhkakäsitteen muodostaminen ankkuroidulla menetelmällä42	
3.3.1 Hallitusohjelma.....	45
3.3.2 Yhteiskunnan turvallisuusstrategia ja kansallinen riskiarvio ..	46
3.3.3 Ulko- ja turvallisuuspoliittinen selonteko	47
3.3.4 Sisäisen turvallisuuden selonteko.....	48
3.3.5 Puolustuselonteko	49
3.3.6 Kansallisesta uhkakuvakäsitteestä johdettu hybridiuhkakäsite49	
4 TUTKIMUSTULOKSET	57
4.1 Hybridiuhkien vertailu tiedustelulakeihin	57
4.2 Tutkimustulokset	62
4.3 Keskeisiä havaintoja hybridiuhkien ja tiedustelulakien vertailusta ..	64
4.4 Tulosten vertailu aiempaan tutkimukseen	67
5 TUTKIMUKSEN JOHTOPÄÄTÖKSET	70
5.1 Tutkimuksen luotettavuudesta ja toistettavuudesta	70
5.2 Jatkotutkimustarpeet ja -mahdollisuudet	72
5.3 Pohdinta	74

LÄHTEET	77
LIITE 1 KANSALLINEN UHKAKUVAKÄSITE HALLITUSOHJELMAN MUKAISESTI	92
LIITE 2 KANSALLINEN UHKAKUVAKÄSITE KANSALLISEN RISKIARVION MUKAISESTI	93
LIITE 3 KANSALLINEN UHKAKUVAKÄSITE ULKO- JA TURVALLISUUSPOLIITTISEN SELONTEON MUKAISESTI.....	94
LIITE 4 KANSALLINEN UHKAKUVAKÄSITE SISÄISEN TURVALLISUUDEN SELONTEON MUKAISESTI.....	95
LIITE 5 KANSALLINEN UHKAKUVAKÄSITE PUOLUSTUSSELONTEON MUKAISESTI	96
LIITE 6 TURVALLISUUSASIAKIRJOJEN MUODOSTAMA KANSALLINEN UHKAKUVAKÄSITE	97

1 JOHDANTO

"Kriiseillä on tapana yllättää ja osoittaa valmistautumista ohjanneet oletukset puutteelliseksi. [...] Tulevaisuudessa edessä voivat olla useat samanaikaiset kriisit, eli niin kutsuttu monihäiriötilanne."

Näin lausuu puolustusministeriön kansliapäällikkönä toiminut Jukka Juusti Turvallisuuskomitean vuosipäivänä 1.2.2021 (Juusti, 2021). Hybridiuhkista puhuttaessa korostuu monesti useat eri vaikutuskeinot, kuten häiriötilanteiden aiheuttaminen sähköverkkoon ja tietoliikenteeseen, yhdistettynä erilaisiin painostaviin toimiin, kuten pakolaisvirtojen aiheuttamiseen – Suomessa onkin arvioitu, että vuonna 2015–16 nähty itärajan pakolaisaalto oli juuri tarkoituksella synnytetty *yllättävä kriisi*. Tällä tutkielmalla on tarkoitus pureutua toimintaamme ohjaaviin oletuksiin, jotka, kuten lainauksessa esitetään, saattavat monesti olla puutteellisia.

Tarkoitus on tutkia ensinnäkin hybridiuhkakäsitettä, ja tämän jälkeen verrata sitä vuonna 2019 voimaan tulleisiin tiedustelulakeihin. Tämän lopputuloksen avulla on tarkoitus muodostaa tietoa siitä, kuinka hybridiuhkiin, tai äskeisen lainauksen *monihäiriötilanteisiin*, voidaan vastata tiedustelulakien avulla. Tässä tutkimusprosessissa selvitetään myös se, mitä tarkalleen ottaen tiedustelulaeilla tarkoitetaan; mitä lakeja se käsittää, mitä toimivaltuuksia nämä lait myöntävät, ja mitkä viranomaiset ovat toimivaltaisia. Tätä tiedustelulakien suomalaista toteutusta verrataan myös muutamiin muihin Euroopan valtioihin, kuinka muissa maissa vastaava lakitoteutus on tehty.

Tarkoitus ei ole luoda käsitystä, että yksinomaan tiedustelulakien toimivaltuuksilla torjuttaisiin nyky maailman monimutkaisia kriisejä tai hybridivaikeuttamista. Tiedustelutoimivaltuudet ovat yksi työkalu viranomaiselle kansallisiin uhkiin ja uhkakuviin vastatessa. Tiedustelulla ei varsinaisesti suoriteta fyysisiä uhkatorjunnan toimia, tai toteuteta vaikkapa ennaltaehkäisevää voimannäyttöä. Tiedustelu on valtiollista, ohjattua tiedonhankinta ja analyysitoimintaa, jolla palvellaan asiakasta, päätöksentekijää (Kivimäki, 2021). Tiedustelun rooli kansallisen turvallisuuden tekemisessä on siis erityisesti se, että sen avulla kansalliset päätöksentekijät voivat saada toimintansa tueksi ja perustaksi lisätietoa

tarjoavaa, objektiivisesti muodostettua, sekä oikea-aikaisesti käyttöön saatavaa tietoa. Mikäli arviot siitä, että tulevaisuuden kriisit voivat olla yhdistelmä monenlaisia häiriötilanteita, on syytä myös arvioida sitä, kuinka tiedustelulakien mukana tulleiden toimivaltuuksien avulla voidaan hankkia tietoa myös tämänkaltaisista kansallisista turvallisuusuhkista.

1.1 Nykypäivän ilmiöitä hybridivaikuttamisesta

Mitä tällainen monihäiriötilanne, laaja-alainen vaikuttaminen, tai kuten tässä alaotsikossa on kirjoitettu, hybridivaikuttaminen voi olla? Esimerkiksi puolustusministeri Antti Kaikkonen Paasikivi-seurassa pitämä puhe 19.1.2021 sisältää monia viittauksia eri vaikutuskeinoihin, kuten tietoverkoissa tapahtuvan vakoiluun tai kybervaikuttamisen kriittiseen infrastruktuuriin. Samalla ministeri kuitenkin näkee myös tarpeen ylläpitää perinteisiä sotilaallisia suorituskykyjä. (Kaikkonen, 2021)

Pian tämän puheen ajankohdan jälkeen Suojelupoliisi tiedotti tunnistaneensa vuonna 2020 Suomen Eduskuntaan kohdistuneen kybervakoiluoperaation kiinalaislähtöisen edistyneen kyberuhkatoimijan toteuttamaksi (Suojelupoliisi, 2021a). Tämä on yksi esimerkki hybridivaikuttamisen keinoista, ja samalla konkreettinen esimerkki kansallisesta turvallisuusuhkasta.

Mikäli ei tarkastella pelkästään suomalaisia esimerkkejä hybridivaikuttamisesta, niin Venäjän valtiojohdon väkivallalla johtamisen muotoja sekä voimapolitiikan toimien olemusta tutkinut Harding (2017) kertoo suomalaisille lukijoille osoittamassaan saatetekstissään lukuisia vaikuttamisen muotoja, joita Venäjä voi käyttää, tai on käyttänyt, Suomea kohtaan. Näiden tavoite on vaikuttaa suomalaiseen valtiolliseen päätöksentekoon siten, että toteutettavat poliittiset päätökset sekä toimintalinjojen asetellut ovat Venäjän etujen mukaisia. Keinoja Harding kertoo olevan ainakin Suomeen kohdistetut kybervakoilu- sekä hyökkäysoperaatiot, maa-alueiden osto Suomen maanpuolustuksen kannalta tärkeiden paikkojen läheltä, toistuvat sotilasalusten tekemät ilmatila- sekä aluevesiloukkaukset, Suomen rajan välittömässä läheisyydessä toimeenpannut suuret sotaharjoitukset, pakolaisvirtojen ohjaaminen Suomeen [tämä liittyi jo mainittuun talvella 2015-16 tapahtuneeseen pakolaisaaltoon Venäjältä Suomeen], sekä venäläisdiplomaattien antamat suorat ukaasit siitä, mitkä ovat Venäjän näkökulmasta aggressivisia turvallisuuspoliittisia päätöksiä; käytännössä siis Nato-jäsenyyden hakemista puoltava päätös. (Harding, 2017, s. 10-11)

Kotimaisessa viranomais- ja poliittisessa diskurssissa on todettu kansallisten uhkakuvien ja turvallisuuskäsitteen suhteen siirtymä yksiselitteisestä monimutkaiseen, ja tämä osoitetaan sekä aihetta käsitellään monessa kohtaa pitkin tätä tutkielmaa. Tässä tutkielmassa käytetään hybridivaikuttaminen ja hybridiuhka -termejä, mutta käytössä on myös muita

termejä, joilla kuvataan samaa aihetta. Ainakin osa näistä muista termeistä kerrotaan ja kuvaillaan tämän tutkielman eri osissa.

1.2 Aiempi tutkimus

Suomalaisia tiedustelulakeja on tutkittu erityisesti pro gradu -tasoisissa opin- näytetöissä. Näissä töissä on otettu eri näkökulmia, muttei kuitenkaan hybridiuhkiin peilaten tai verraten. Tiedustelulainsäädäntöä on näissä töissä liitetty muun muassa kyberturvallisuuteen (Tanner, 2019), avointen lähteiden tiedusteluun (Siljoranta, 2020) sekä tiedustelun valvonnan toteutukseen (Pekola, 2018). Lisäksi pro graduissa on tutkittu tiedustelulakien valmistelua, painottuen tutkimaan tiedustelulakeja valmistelleiden työryhmien tuottamiin teksteihin, muun muassa Mannosen (2020), Heleniuksen (2020), Heinosen (2019), Havulinna (2018), Leppäsen (2018) sekä Kurttilan (2015) toimesta.

Opinnäytetöiden lisäksi tähän lukuun on valittu esitettäväksi muutamia tuoreimpia teoksia keskeisiltä organisaatioilta, jotka toimivat kokonaisturvallisuuden alueella. Teemat *turvoallisuus*, *hybridiuhkat*, *uhkakuvat* tai *tiedustelu* tuottavat tietohauissa kosolti hakutuloksia, joten kaikkea löytyvää tutkimusta ei ole relevanttia listata. Eli paneudutaan keskeisimpiin teoksiin, jotka ovat pääosin kotimaista tämän tutkielman aiheeseen liittyvää tutkimusta. Osaa seuraavaksi esiteltävistä teoksista vertaillaan tämän tutkielman tuloksiin tutkielman viimeisessä pääluvussa, yhteenveto- ja pohdintaluvussa, ja nämä teokset ovat siis sellaisia, jotka eivät ole tutkimusaineistona tutkielman hybridiuhkakäsitettä muodostettaessa.

Valtioneuvoston toimeksiannosta on tutkittu kansallisen turvallisuuden olemusta aivan hiljattain (Lonka ym., 2020), ja kulttuurin ja yhteiskunnan tutkimuksen alalla on tutkittu tutkimusartikkelin muodossa valtiollista kybertoimintaympäristöämme sivuten tiedustelulainsäädäntöä (Jansson & Sihvonen, 2018). Helsinkiin sijoitettu EU:n ja Naton kanssa läheistä yhteistyötä tekevä Euroopan hybridiuhkien torjunnan osaamiskeskus tekee paljon nimensä mukaista tutkimustyötä, kuten tämän tutkielman kirjoitushetkellä julkaistu hybridiuhkakäsitettä viitekehystävä ja teoretisoiva tutkimus (Giannopoulos, Smith & Theocharidou, 2021).

Myös Turvallisuuskomitea, joka toimii puolustusministeriön yhteydessä tehtävänään avustaa valtioneuvostoa ja ministeriöitä kokonaisturvallisuuteen liittyvissä asioissa, tuottaa tietoa tämän tutkielman aihealueesta. Turvallisuuskomitean viimeisin, puhtaasti hybridiuhkiin keskittyvä julkaisu on vuodelta 2016, johon on koottu aihealueen eri asiantuntijoiden puheenvuoroja sekä organisaatioiden esityksiä (Nevaste, 2016). Näihin tässä tekstikappaleessa mainittuihin lähteisiin ei kuitenkaan ole perehdytty tämän opinnäytetyön tutkimusvaiheessa, vaan vasta yhteenvetovaiheessa, jotta ankkuroidun tutkimusmenetelmän perusidea ei katoa; tutkimusmetodin henkeen kuuluu pidättäytyä valitussa tutkimusaineistossa, joka kuvaa tutkimuskohteena olevaa uutta, vähän tutkittua ilmiötä. Valittua tutkimusaineistoa koodaamalla muodostetaan tutki-

muksen teoria, ja koodaamisen aikana, tai ainakaan sen alkuvaiheessa, ei tutkijan tulisi lukea muuta tutkittavaa kohdetta käsittelevää kirjallisuutta. Tämä muusta aineistosta pidättäytyminen takaa tutkimuksen toistettavuuden ja varmistaa sen, että teorian voidaan sanoa muodostetun juuri valitusta aineistosta, eikä muodostukseen ole päässyt vaikuttamaan muut tutkittavaa ilmiötä kuvaavat aineistot. (Silvonen & Keso, 1999, s. 90)

Kansainvälistä tutkimustietoa tämän opinnäytetyön aiheeseen on saatavilla muun muassa ihmisoikeusnäkökulmasta, jossa keskiöön nostetaan kansallisen turvallisuuden ja kansalaisten valvonnan välinen problemaattinen suhde (Council of Europe, 2016). Digitaalisen ajan tiedustelusta ja tiedonhankinnasta on kirjoittanut muun muassa Donohue (2016), ja samasta aiheesta, mutta eurooppalaisessa viitekehyksessä, on muun muassa Wrightin ja Kreisslin teos (2014). Nämä eivät ole ainoita tieteellisiä teoksia aiheesta, ja esimerkiksi kaksi muuta teosta nostetaan esiin tiedustelulakien kansainvälisen tarkastelun alaluovussa 2.3 (Jong, Duyvesteyn & Reijn, 2014; Omand & Phythian, 2018).

Teoreettista pohdintaa valtiollisen vaikuttamisen uusista keinoista, aina diplomatiasta voimapolitiikkaan ja sodankäyntiin, on luettavissa muun muassa Libickin (2007), Abbottin (2010) sekä Singerin ja Brookingin (2018) teoksista. Miksi tutkielmaan liittyvää aiempaa aineistoa mainitaan *valtiollisen vaikuttamisen* kentästä, niin kuten myöhemmin tässä tutkielmassa perustellaan, kansallisia uhkakuvia käsitellessä, siihen olennaisena osana kuuluu analysoida valtion ympäristöä, eli mitkä toimijat ja tekijät muodostavat uhkapotentiaalia meitä kohtaan. Vaikka uhkat ovat monimuotoistuneet, yksi olennainen toimija on edelleen toiset valtiot.

Ja toista tämän tutkielman pääteemaa, eli hybridiuhkia, on myös tutkittu, ehkä jopa enemmän kuin tiedustelulakeja. Mutta mikäli nämä tutkimukset rajataan käsittämään vain tieteelliset julkaisut, eli ne pohjautuvat alan aiempaan tutkimukseen ja pyrkivät tuottamaan uutta tietoa vaikkapa teorian muodossa, ei tekstejä ole kovinkaan paljoa puhtaasti suomalaisesta näkökulmasta. Valtaosassa tekstejä viitekehys on kansainvälinen (ks. esim. Giannopoulos, Smith & Theocharidou, 2021; Hoffman, 2009; Smith, 2019). Näissä tutkimuksissa pyritään konseptualisoimaan ja käsitteellistämään hybridiuhkia teoriatasolla, jolloin muodostetun tiedon käyttökelpoisuus ja selitysvoima olisi mahdollisimman universaali.

Edelleen mikäli hybridiuhkia käsittelevät tekstit ovat enemmän käytännönläheisyyteen suuntautuneita, vaikkapa jotain tiettyä toimijaa varten laadittuja (kuten esim. tämä NATO:n tarpeisiin tehty tutkimus: Lasconjarias & Larsen, 2015), voivat ne olla liian suppeasta näkökulmasta laadittuja ollakseen käytettäviä muussa tutkimustyössä. Nämä tekstit siis eittämättä ovat käyttötarkoitukseensa nähden relevantteja, mutta eivät välttämättä täytä tieteellisen tiedon vaatimuksia, kuten muun muassa Myers (2019, s. 13) jaottelee käytäntöön ja tieteeseen suuntautuneiden tutkimuksien erot laadullisessa tutkimuksessa.

1.3 Tutkielman tavoite, tutkimuskysymykset ja -rajaukset

Tämän tutkielman tavoitteena on konkretisoida hybridiuhkakäsite Suomen valtiollisten tekstien kautta ja selvittää, voiko nykymuotoisilla tiedustelulaeilla hankkia tietoa niistä kansallisista turvallisuusuhkista, jotka hybridiuhkat synnyttävät. Hybridiuhkakäsitteen ei tule olla paikoilleen sementoitunut, vaan päinvastoin, se vaatii jatkuvaa tarkastelua eri näkökulmista.

Miksi näin? Nopeasti tapahtunut, fyysistä maailmaamme koskettava jatkuva teknologinen kehitys on tuonut vallankumouksellisia piirteitä ihmiskuntaa kohtaan (tästä lisää luvussa 4.3), joten myös vaikuttamisen keinot elävät tässä samassa jatkuvan muutoksen tilassa. Tässä tutkielmassa tarkastellaan hybridiuhkia valtiollisten tekstien lisäksi tiedustelulakien näkökulmasta.

Tutkielman pääkysymys on asetettu muotoon:

- kuinka kattavasti suomalaisten tiedustelulakien mukaisilla valtuuksilla voivat toimivaltaiset viranomaiset vastata hybridiuhkiin?

Pääkysymykseen vastaamista tukemaan ja vastauksen laatua parantamaan esitetään seuraavia apukysymyksiä. Näihin apukysymyksiin vastaamalla eritellään tutkielman keskeistä käsitteistöä sekä tiedustelulakeja. Tutkielman apukysymykset ovat aseteltu muotoon:

- mitä hybridiuhkat ovat ja miten tämä käsite määritellään suomalaisessa kansallisen tason asiakirjoissa?
- mitä lakeja tiedustelulait käsittävät? Mitä toimivaltuuksia viranomaisille tuli verrattuna aikaan ennen tiedustelulakeja?

Apukysymyksillä on tarkoitus ensinnäkin konkretisoida hybridiuhkien käsitämä uhkaskaala. Kyseinen hybridiuhka -termi on laajalti käytetty, mutta mitä kaikkia uhkia siihen spesifisti sisältyy ja painotetaanko joitain uhkia enemmän kuin toisia? Toisekseen muodostamalla yleinen suomalainen hybridiuhkakäsite vastataan tämän pääluvun osassa 'aiempi tutkimus' esitettyyn dilemmaan siitä, että nykyiset hybridiuhkakäsitteet ovat useasti luotu jonkin tietyn toimijan tarvetta varten, eikä yleisesti päteviksi. Esimerkiksi paljon käsitteellistämistä löytyy sotilaallisista tarpeista lähtöisin, kun on tutkittu vuonna 2014 alkanutta Ukrainan konfliktia. Hybridiuhkien määrittäminen on olennaisen tärkeää tutkielman pääongelmaan vastaamiseksi. Mikäli tämä määrittely tehdään heppoisesti, aiheutuu siitä se, ettei tutkielmassa voida luotettavasti vastata siihen, kuinka tiedustelulaeilla voidaan hybridiuhkiin vastata. Hybridiuhkatarkastelussa etsitään myös uhkia, joilla on tällä hetkellä pieni painotus tai ovat jollain tavalla puutteellisesti tunnistettuja, mutta joilla on potentiaalia kehittyä nykyistä vakavammiksi uhkiksi.

Toisen apukysymyksen avulla kuvataan ensinnäkin tiedustelulait, jotta tiedetään selvästi ja tarkkarajaisesti, mihin lakiteksteihin hybridiuhkia peilataan. Tämä apukysymys on erityisellä tarkoituksella kaksiosainen, jotta kysymyksessä ilmenee ajallinen ulottuvuus. Kuten tiedustelulakeja esiteltäessä huomataan, ne ovat vasta vuoden 2019 kesällä saatettu voimaan, eli ovat lakeina siis varsin nuoret. Jotta tätä vasta syntynyttä nykyhetken tilannetta voi tiedustelutoiminnan kannalta syvällisesti ymmärtää, tutkielmassa kuvataan, miten tiedustelulait ovat muuttaneet tiedustelutoiminnan mandaatteja. Mitä tiedustelulait ovat mahdollistaneet? Mitä sellaista voimme nyt tehdä kansallisen turvallisuuden eteen, mikä ei ollut mahdollista ennen nykymuotoista lainsäädäntöä? Tämän määrittelyn avulla voi lisäksi tehdä johtopäätöksiä siitä, mitä kansallisia turvallisuusuhkia nähtiin lakeja säättäessä relevanteiksi nykypäivänä. Ja lopuksi, tutkielmassa muodostettuun hybridiuhkakäsitteeseen voi peilata erityisellä tarkkuudella niitä tiedustelun mandaatteja, mitkä tulivat uusina voimaan vuonna 2019; voidaan kysyä, onko uusilla tiedustelumandaateilla todella pystytty vastaamaan nykyhetken hybridiuhkiin.

Koska tutkielmassa on paljon eri käsitteitä, on tutkimusrajaukset pitänyt tehdä huolellisesti, jottei tutkielman mitta ja aihealue paisu liian isoksi. Päätutkimuskysymyksen mukaisesti tutkielmassa tarkastelu rajataan vain suomalaista lainsäädäntöä ja yhteiskuntaa koskevaksi. Vertailun vuoksi tutkielmassa esitetään muutamia tapausesimerkkejä länsimaista, kuinka tiedustelulainsäädännön ja monimuotoisten sekä osin vaikeasti tulkittavien uhkien – eli hybridiuhkien – välinen suhde on muodostettu. Samalla, ja näiden kuvausten avulla, osoitetaan, että kansallisen tiedustelun järjestäminen, ja tiedonhankinnan laajuus, eivät suinkaan ole keskustelua ja probleemaa herättäviä teemoja vain Suomessa, vaan kyseessä on laajempi dilemma ainakin länsimaisissa demokratioissa.

Edelleen päätutkimuskysymyksen vastaus on muodostettu tarkastelemalla vain viranomaisten, ja tarkemmin tiedustelutoimivaltuuksilla toimivien viranomaisten, työtä kansallisen turvallisuuden eteen. Suomalaisessa kokonaisturvallisuuden konseptissa turvallisuuden tuottajia ovat viranomaisten lisäksi, ja rinnalla, niin elinkeinoelämä, eri järjestöt, yhteisöt kuin me ihmiset yksilöinä (YTS, 2017, s. 7–8), ja tutkielmaa lukiessa tulee ottaa huomioon näiden muiden turvallisuuden tuottajien poissaolo tutkimuksen pääongelmaan vastattaessa. Tosin hybridiuhkakäsite tutkielmassa muodostetaan kattavasti eri lähteitä analysoimalla, eli sen muodostamisessa ei jätetä mitään osa-alueita pois. Lisäksi kun muodostettua hybridiuhkakäsitettä peilataan tiedustelulakeihin päätutkimuskysymyksen mukaisesti, on toimivaltaisena tahona pelkästään tiedustelua toteuttavat viranomaiset, joten tutkimuksen vastauksen luotettavuus ei heikene näiden muiden turvallisuustoimijoiden ulos sulkemisen myötä.

Tutkielmassa ei paneuduta käytännön tiedustelutyöhön ja -menetelmiin niiden ollessa varsin tiukasti salassa pidettäviä asiakokonaisuuksia, vaan tiedustelua tarkastellaan tiedustelulainsäädännön kautta. Tätä valintaa tiedustelulakien kautta tehtävään tarkasteluun ei ole muodostettu siksi, että se olisi ainoa julkisen tiedon väylä tiedustelun tutkimiseen, vaan ennen kaikkea siksi, että tiedustelulait ovat Suomessa varsin nuoret, tutkielman tekohetkellä vain muu-

tamia vuosia vanhat. Näin tuoreiden ja ensimmäistä kertaa säädettyjen lakien toimivuutta alati muuttuvassa maailmassa tulee tarkastella monipuolisesti ja kriittisesti, ja tämä tutkielma pyrkii kantamaan kortensa siihen kekkoon.

Tiedustelulakien osalta tutkimuksen tarkastelusta rajataan ulos tiedustelun laillisuusvalvontaan liittyvä laki esitöineen. Tämä laki kyllä esitellään tutkielman aikana relevanteissa kohdissa, jottei lukijalle tule väärää ymmärrystä siitä, etteikö tiedustelutoiminnan laillisuutta valvottaisi. Kuitenkaan tutkielmassa ei perehdytä tiedustelun laillisuusvalvonnan järjestämiseen samalla tarkkuudella kuin tiedustelua toteuttavien viranomaisten toimintaan, koska ensinnäkään laillisuusvalvontatarkastelu ei toisi juurikaan lisäarvoa tutkimuskysymyksiin vastattaessa, ja toisekseen tutkielman rajatusta pituudesta täytyy joitain osia karsia pois, jotta ydinteemaan voidaan pureutua tarpeeksi kattavasti.

2 TIEDUSTELUN ROOLI KANSALLISEN TURVALLISUUDEN TEKIJÄNÄ

Tässä pääluvussa keskitytään tutkimusrajausten mukaisesti kotimaiseen tiedustelutoimintaan tiedustelulakien kautta tarkasteltuna. Poikkeuksen tekee alaluku 2.3, jossa katsauksenomaisesti perehdytään eräiden muiden valtioiden tapaan järjestää oma valtiollinen tiedustelutoiminta. Kyseinen alaluku on tietoisesti sijoitettu suomalaisten tiedustelulakien analyysin ja tiedusteluviranomaisten esittelyn jälkeen, jotta kansainvälistä näkökulmaa voi peilata kotimaiseen tapaan järjestää tiedustelutoiminta. Pääluku päätetään katsaukseen siitä, kuinka ajattelumme turvallisuudesta on yhteiskunnassamme muuttunut niin sanotun laajentuneen turvallisuuskäsityksen myötä. Tämä laajentunut tapa ajatella turvallisuutta toimii siltana hybridiuhkakäsitteen synnylle, ja pääluku päätetäänkin alalukuun siitä, kuinka eräät suomalaiset viranomaiset määrittelevät hybridiuhkakäsitettä - vai käytetäänkö kyseistä termiä ollenkaan.

Tässä pääluvussa esitetään faktatietoa tiedustelutoiminnasta, ja tutkielman tekijä ei ole tässä luvussa luonut tietoa - esimerkiksi yhdistänyt eri lähteistä synteesisomaisesti omia johtopäätöksiä - tai tehnyt oletusten kautta yhteenvetoja asioiden tilasta. Tämä faktoissa pidättäytyminen ja tekstien varsin rajattu tulkinta on tietoinen valinta, sillä seuraavassa pääluvussa toteutetaan tämän tutkielman varsinainen tutkimusaineiston koodaus ja käsitteiden muodostaminen, joista hybridiuhkakäsitettä peilataan muun muassa tämän pääluvun antiin tiedustelulakien toimivaltuusasioiden osalta. Mikäli tässä pääluvussa esitettäisiin pitkälle meneviä tutkijan omia johtopäätöksiä, joihin sitten tulevaa vertailua tehtäisiin, olisi vaara tutkimustulosten vääristymiselle siinä mielessä, että tutkijan omat ajatukset saattaisivat olla liian isossa roolissa.

Johtopäätösten puute ei kuitenkaan tarkoita, että tämän pääluvun merkitys olisi vähäinen. Tiedustelulait ovat Suomessa varsin nuoret, ja vielä viime vuosina niiden asemasta käytiin varsin perustavanlaatuaistakin julkista debattia - kuka tiedustelutoimintaa valvoo, ovatko kaikki tiedustelumandaatit tarpeellisia, kenelle mitäkin tietoa luovutetaan. Näin on syytä alaluvussa 2.2 määrittää tämän hetken tilanne, mitä konkreettisesti on muuttunut

tiedustelulakien voimaantulon myötä, eli mitä viranomaistoiminnan mandaatteja tiedustelulait ovat tuoneet. Ja jotta voidaan syvällisemmin ymmärtää mitä tiedustelulait ovat, kuvataan samassa luvussa myös tiedustelulakien valmistelutyö.

Tämä pääluke aloitetaan kuitenkin kuvaamalla suomalaisten tiedustelulakien mukaista hallinto- ja toimivaltaa käyttävät viranomaiset, eli niin sanotut tiedusteluviranomaiset. Kuten tiedustelulakeja kertovassa alaluvussa, myös tässä tiedusteluviranomaisiin liittyvässä luvussa kerrotaan lähihistoriaa. Painotus on tosin siviilitiedusteluviranomaisen historian kerronnassa, koska 2010-luvulla tapahtunut tiedustelulakityö vaikutti erityisesti kyseisen viranomaisen tehtäviin sekä organisatoriseen sijoittumiseen omalla hallinnonalallaan (sisäministeriö). Tällä lähihistorian kerronnalla ja analyysillä niin viranomaisten kuin tiedustelulakien osalta vastataan myös tutkielman toiseen apukysymykseen, eli mitä lakeja tiedustelulait käsittävät ja mitä toimivaltuusmuutoksia nämä lait toivat.

2.1 Tiedusteluviranomaiset Suomessa

Sotilastiedustelun viranomaistaho, siis sotilastiedustelulainsäädännön mukaista julkista valtaa käyttävä toimija, on Puolustusvoimien Tiedustelulaitos sekä pääesikunnan sotilastiedusteluun määrätyt virkamiehet (laki sotilastiedustelusta, 590/2019, 11 §). Sotilastiedustelun johtamishierarkian ylimmällä tasolla on ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin muodostama elin (ns. *tp-utva*), joka antaa ylimmän tason ohjauksen sekä painopisteet sotilastiedustelulle. Tämä painopisteittäminen tapahtuu vuosittaisella syklillä, mutta samalla ylläpidetään valmius lyhytaikaiseen painopisteiden mukauttamiseen (Puolustusvoimat, 2021a, s. 15–16). Käytännössä painopisteittäminen vuosittain rytmitys etenee siten, että tammikuussa tarkastellaan edellisen vuoden tuloksellisuutta, ja aloitaan seuraavan vuoden valmistelu. Syksyllä seuraavalle vuodelle laaditut painopisteet menevät *tp-utvan* käsittelyyn, josta ne syksyn aikana jalkautuvat vastuuministeriöihin, eli puolustus- sekä sisäministeriöön (Pöysti, 2021, s. 6).

Sotilas- ja siviilitiedusteluorganisaatiot ovat relevantein osin mukana tässä edellä kuvatussa ylimmän tason työssä. Käytännössä tämä työ voi ilmetä muun muassa tilanteessa, jossa *tp-utva* asettaa yleisellä tasolla kansallisen tiedustelun prioriteetteja, ja tiedusteluorganisaatiot osallistuvat työhön, jossa näitä tiedusteluvastuita jaetaan siviili- ja sotilaspuolen kesken (Ohra-aho, 2019, 27:00).

Puolustusministeriö on seuraava organisatorinen taso, joka puolestaan käskää sotilastiedustelulle (Pääesikunnalle) edellä mainitut painopisteet sekä ohjaa muutoinkin hallinnollisesti sotilastiedustelua (laki sotilastiedustelusta, 590/2019, 12 ja 13 §). Hallinnollinen ohjaus tarkoittaa muun muassa tulosoajasta ja resurssien käytön suunnittelua ja jakoa Puolustusvoimallisella tasolla (HE, 203/2017, s. 36). Puolustusministeriö ei siis ota kantaa siihen, millä

tiedustelumenetelmillä mihinkin prioriteettiin tai painopisteeseen tulee tiedonhankinta tehdä (Puolustusvoimat, 2021a, s. 16).

Seuraava organisaatiotaso on Pääesikunta, jossa korkein asema sotilastiedustelun suhteen on Pääesikunnan operaatiopäälliköllä, sillä sotilastiedustelu on osa Puolustusvoimien operatiivista toimintaa (Puolustusvoimat, 2021a, s. 19). Sotilastiedustelun varsinaisen toiminnan, kuten toimivaltuusasioiden ja Puolustusvoimien tiedustelulaitoksen ohjauksen, osalta ylintä päätösvaltaa käyttää Pääesikunnan tiedustelupäällikkö (Hakonen, 2020a, s. 9). Pääesikunnassa sotilastiedusteluorganisaatioon kuuluu myös tiedusteluosasto, joka muun muassa koordinoi sotilastiedustelun prosessia, vastaa tiedustelujärjestelmien kehittämisestä, sekä toimii tahona, joka antaa valtiolliselle päätöksentekotahoille tarvittavia ennakkovaroituksia. Nämä ovat otteita kyseisen organisaation tehtäväkirjosta, joilla alleviivataan heidän päätehtävää: vastata sotilastiedustelun kokonaisuudesta puolustusvoimissa (Puolustusvoimat, 2021b).

Edelleen alemmalle organisaatiotasolle siirryttäessä, on Pääesikunnan alaisuudessa Puolustusvoimien tiedustelulaitos. Tiedustelulaitoksen tehtäviä tarkastellessa sen toiminnan voi mieltää kuuluvan tiedusteluvalvontavaltuutetun käyttämin termein ”operatiiviseksi tiedusteluksi”, joka tarkoittaa muun muassa sitä, että kyseisellä toiminnalla hankitaan kansallisen turvallisuuden ylläpidon edellyttämiä yksittäisiä tietoja (Hakonen, 2020a, s. 7). Edelleen tiedusteluvalvontavaltuutettu Hakonen tarkentaa kolumnissaan operatiivisen sotilastiedustelun tarkoitusta; sitä kohdistetaan vieraan valtion sotilaalliseen toimintaan liittyviin konkreetisiin kohteisiin (Hakonen, 2020b). Tiedustelulaitoksen tehtäviin siis kuuluu muun muassa Suomen sotilaallisen toimintaympäristön seuranta, arviointi ja raportointi, sekä tarjota paikka- ja olosuhdetietopalveluita (Puolustusvoimat, 2021a, s. 19), eli juurikin tiedon muodostaminen konkreettisista ja yksilöitävissä olevista kohteista. Myös puolustusvoimien puolustushaarat (maa-, meri- ja ilmavoimat) toteuttavat omaa tiedusteluansa, mutta niiden päätarkoitus on palvella oman puolustushaaran operatiivista toimintaa sekä siihen liittyvää suunnittelutyötä, eivätkä nämä puolustushaarojen tiedustelutoimialat ole sotilastiedustelun tarkoittamia tiedusteluviranomaisia. Poikkeuksen tähän muodostaa radiotaajuinen signaalitiedustelu, jossa puolustushaarojen suorituskyvyt voivat, sotilastiedustelun päätöksellä, kohdistaa signaalitiedustelua Suomen alueen ulkopuolisista laitteista tuleviin ja niistä lähteviin radioaaltoihin (laki sotilastiedustelusta 590/2019, 60–61 §). Sotilastiedusteluorganisaatio on nyt esitelty ylhäältä päin alkaen, ja seuraavaksi tarkastellaan siviilitiedustelun järjestämistä Suomessa.

Siviilitiedustelumandaattia käyttää Suojelupoliisi, joka sijoittuu organisatorisesti sisäministeriön kansallisen turvallisuuden yksikön alaiseksi turvallisuus- ja tiedustelupalveluksi. Aina vuoteen 2016 asti Suojelupoliisi organisaationa sijoittui sisäministeriön poliisitoimen alle, jonka toimialan ylimpänä hallintoviranomaisena on Poliisihallitus. Näin Suojelupoliisi kuului yhtenä valtakunnallisista poliisiyksiköistä (muiden ollessa Keskusrikospoliisi ja

Poliisiammattikorkeakoulu) Poliisihallituksen alaisuuteen. (HE 364/2014, s. 4; laki poliisin hallinnosta 110/1992, 1 §)

Suojelupoliisi perusti toimintansa ennen tiedustelulakeja pitkäli poliisin niin sanottuihin yleislakeihin, eli poliisi-, esitutkinta- ja pakkokeinolakiin (HE 202/2017, s. 6). Oli siis luonnollista, että Suojelupoliisia ohjattiin kuten muutakin poliisitoimintaa. Tiedustelulakien valmistelutyössä lausuttiin kuitenkin muun muassa vuoden 2014 lopulla ylimmän poliisijohdon toimesta, että Suojelupoliisin eräät tehtävät, kuten strategisten ilmiötason muutosten analysointi sekä vastaavan tarkastelutason uhka-arvioiden luonti, ja niistä poikivat tiedonhankintatarpeet eivät voi tulla täytetyksi rikosperusteisilla toimivaltuuksilla. Samassa poliisijohdon kommentissa ratkaisuna esitettiin Suojelupoliisin toimivaltuuksien tarkastelua erillään muusta poliisitoiminnasta. (Nordström ym., 2015, s. 139)

Samana vuonna 2014 hallitus antoi lakiesityksensä Suojelupoliisin siirtämisestä suoraan sisäministeriön alaisuuteen ja ohjattavaksi, sen säilyttäessä poliisiyksikön statuksen. Tätä muutosta perusteltiin kansallisen uhkakuvakentän monimutkaistumisella sekä valtion sisäisen ja ulkoisen turvallisuuden rajan hämartyksellä, joista kehityskuluista on seurannut se, että Suojelupoliisin tehtäväkentässä korostuu tiedustelullinen toiminta. Hallitus näki tuolloin vuonna 2014, että Suojelupoliisin tehtävät eroavat muusta poliisista siinä määrin, että rikostutkinta ei enää ole sen päätehtävä. Vaikka hallitus totesikin, että silloisessa nykytilassa, eli Poliisihallituksen alaisuudessa, Suojelupoliisilla on varsin itsenäinen asema ja käytännössä se kansallisen turvallisuuden asioissa kommunikoi suoraan ylimmän valtiosijon ja muiden tarpeellisten tahojen kanssa ohi virkatien, selkeyttäisi siirto sisäministeriön alaisuuteen Suojelupoliisin organisatorista asemaa. Myös toiminta tehostuisi, kun valtiosijon voisi suoraan ministeriön kautta antaa tarvittavan strategisen ohjauksen ja painopisteet. (HE 346/2014, s. 3-10)

Näin ollen jo mainitusti Suojelupoliisi siirtyi vuoden 2016 alussa suoraan sisäministeriön alaisuuteen, asettuen sisäministeriön poliisiosaston ohjattavaksi. Tämä hierarkiasuhde säilyi aina vuoden 2019 kesäkuuhun asti, jonka jälkeen Suojelupoliisin toiminnan ohjaus siirrettiin sisäministeriön vasta perustettuun kansallisen turvallisuuden yksikköön. Kansallisen turvallisuuden yksikön muut tehtävät ovat muun muassa siviilitiedusteluasioiden käsittely sekä, nimensä mukaisesti, kansallista turvallisuutta koskevien asioiden käsittely. Siten oli pelkästään luontevaa, että Suojelupoliisi siirrettiin tämän kaltaisen yksikön ohjattavaksi sillä samalla hetkellä, kun tiedustelulait astuivat voimaan. (Sisäministeriön asetus sisäministeriön työjärjestyksestä annetun asetuksen muuttamisesta, 757/2019)

Välittömästi Suojelupoliisin vuoden 2016 vuosikirjassa Suojelupoliisin päällikkö Antti Pelttari kuvasi tämän organisatorisen muutoksen vaikuttaneen positiivisesti Suojelupoliisin itsenäiseen asemaan. Muutoksen myötä oli virasto saanut vapaammat kädet toimintansa uudistamiselle. Edelleen Pelttarin mukaan silloisen uudistusstrategian keskiössä oli Suojelupoliisin kehittäminen kohti suomalaista valtiollista siviilitiedustelupalvelua, jonka keskiössä on

ennakoivan ja merkityksellisen tiedustelutiedon tuottaminen kansallisen turvallisuuden takaamiseksi. (Suojelupoliisi, 2017, s. 5)

Näin Suojelupoliisi on kehittynyt hallinnollisesti rikosperusteisia toimivaltuuksia käyttävästä poliisiyksiköstä kohti valtiollista siviilitiedustelupalvelua, poliisiyksikön juuria ja taustaa unohtamatta (vuoden 2016 vuosikirjassa viraston päällikkö Peltari korostaa, että muutoksesta huolimatta poliisiyksikön status halutaan säilyttää Suojelupoliisin pohjana). Tuoreimmassa, vuoden 2020 vuosikirjassaan, Suojelupoliisi kuvaakin jo perustehtävänsä muun muassa sanoilla ”valtionjohdon ja viranomaisten palveleminen tiedustelutiedolla”, sekä ”uhka-arvioiden tuottaminen” [eri asiakkaille] (Suojelupoliisi, 2021b, s. 15–16). Tässä kappaleessa kuvattu organisatorinen ja hallinnollinen muutos ei ole tapahtunut ilman merkittäviä lakimuutoksia, joten tässä luvussa ei voitukaan välttyä viittauksista lakimuutoksiin. Näinpä luontevana jatkumona tiedusteluviranomaisten esittelyn jälkeen perehdytään itse tiedustelulakeihin, niiden valmisteluvaiheesta alkaen.

2.2 Tiedustelulait – mitä ne ovat ja mitä ne toivat?

2.2.1 Tiedustelulakien syntyminen

Nykymuotoisten suomalaisen lainsäädännön tiedustelulakien valmistelun voidaan katsoa saaneen alkusysäyksen, ainakin julkisen sellaisen, vuoden 2013 kyberturvallisuusstrategian myötä (Eduskunta, 2019). Tässä strategiassa nähdään tarve lainsäädäntötyölle, jotta viranomaisten tiedonhankinta ja tilannekuva yhteiskunnan elintärkeiden toimintojen uhkista sekä kansallisesta turvallisuudesta on niin kattavaa, että sillä voi vastata monimuotoistuneisiin uhkiin (Valtioneuvosto, 2013, s. 8, 10).

Kun kyberturvallisuusstrategia julkaisiin tammikuussa 2013, alkoi strategian mukainen työ välittömästi. Puolustushallinto aloitti joulukuussa 2013 työryhmävetoisesti kansainvälisen oikeuskäytännön tarkastelun, oman kansallisen lainsäädäntömme analyysin sekä saadakseen vertailukohtia, eräiden muiden valtioiden kansallisen lainsäädännön tutkimisen (kyberturvallisuuteen liittyvien lainkohtien osalta) (Puolustusministeriö, 2013). Vaikka lainsäädäntötyön painopiste oli strategian mukaisesti kybertoimintaympäristön uhkiin vastaamisessa, niin esimerkiksi puolustusministeriön laatimassa valmistelutyöryhmän asettamispäätöksessä lausuttiin sen työn tavoitteeksi sanamuodoin: ”tavoitteena on selvittää turvallisuusviranomaisten tiedonhankintaa koskevat toimintaedellytykset erityisesti kybertoimintaympäristön kautta”, ja ”tiedonhankintaa koskevat nykyiset toimivaltuudet ja niiden kehittämistarpeet” (Puolustusministeriö, 2013). Eli vaikka kimmoke lainsäädäntötyön kehittämiseen tuli kansallisesta kyberturvallisuusstrategiasta, aloitettiin lakivalmistelu kokonaisvaltaisella lähestymistavalla kansalliseen turvallisuuteen, kybernäkökulma kuitenkin painopisteessä.

Puolustusministeriön asettaman työryhmän rinnalla, siis osin samoja kysymyksiä käsitellen, toimi sisäministeriön asettama Suojelupoliisin hallinnollista asemaa, tulosoajasta ja valvontaa käsittelevä työryhmä (HE 202/2017, s. 7). Kun jo edellisluvussa kerrottiin Suojelupoliisin hallinnollisen aseman muutoksesta poliisitoimen ja sisäministeriön alaisuudessa, niin osaltaan myös tämä työryhmätyö toimi pohjana näiden muutosten tekoon. Vuoden 2014 lopulla annetun hallituksen esityksen Suojelupoliisin aseman muuttamisesta (HE 364/2014) tausta-aineistoina toimi muun muassa tämän työryhmän laatima aineisto.

Mutta kun siis hallituksen esityksessä Suojelupoliisin muutosta perusteltiin erityisesti tiedonhankinnan kyvykkyyden parantamisella (HE 364/2014, s. 8), niin tässä työryhmässä esitettiin muutostarpeeksi myös laillisuusperusteet. Oli havaittu, että tiedonhankinta monista uhkista on käytännössä mahdotonta rikosperusteisilla toimivaltuuksilla, joten tässä kohtaa toimivaltuuksien laajentaminen nähtiin ongelmallisena, mikäli esitutkintatoimivaltuudet säilyvät samalla muuttumattomana. Tämä sisäministeriön asettama työryhmä julkaisi loppuraporttinsa vuoden 2014 jälkimmäisellä puoliskolla, jossa työryhmä lausui, että mikäli Suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulee oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita Suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittamista (Sisäministeriö, 2014, s. 53).

Vuonna 2014 kansallisen lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista sai edelleen lisäpontta, kun Turvallisuuskomitea (2014) julkaisi kyberturvallisuusstrategian toimeenpano-ohjelman. Vaikka Turvallisuuskomitea itsessään on perustettu puolustusministeriön yhteyteen, se käyttää poikkihallinnollista mandaattia, joten kyseinen elin voi antaa toimenpidesuosituksia yli virasto- ja hallintorajojen (Valtioneuvoston asetus Turvallisuuskomiteasta 77/2013, 2 §). Näinpä toimenpideohjelmassa suositellaankin, että tiedonhankintakyvyn parantamiseen liittyvään lainsäädäntötyöhön osallistuisi kattava osallistujajoukko. Osallistujat olisivat Tasavallan presidentin kansliasta, eri ministeriöistä, ja virastotasolla Poliisihallitus, Suojelupoliisi ja puolustusvoimien Pääesikunta (Turvallisuuskomitea, 2014, s. 39–41).

Valmistelutyö 2010-luvun neljänä ensimmäisenä vuotena oli siis varsin kattavaa, mutta painopisteessä pysyi kybernäkökulma sekä tietoverkoissa esiintyvien, sekä sitä kautta toteutettavien, uhkien torjunta. Aiemmin tässä luvussa mainittu Puolustusministeriön asettama lainsäädäntöä tarkasteleva työryhmä (Puolustusministeriö, 2013) sai työnsä valmiiksi vuoden 2014 loppuun mennessä, ja julkaisi loppumietintönsä tammikuussa 2015 (Puolustusministeriö, 2015). Jatkotoimenpiteinä työryhmä ehdotti tarvittavien lainsäädäntöhankkeiden aloittamista, joista osassa valmisteluvastuussa olisi sisäministeriö, ja osassa puolustusministeriö. Tämän työryhmän loppupäätelmissä ei enää keskitytä pelkästään kyberteemaisiin näkökulmiin tai painopisteisiin, vaan kansallisen turvallisuuden kannalta välttämättömästä tiedustelutiedosta puhutaan sekä tietoliikennetiedustelun että ulkomaantiedustelun alaluvuilla. Johtopäätöksissä käytetään paljon konditionaalimuotoja, mutta viesti lukijalle näyttäytyy kuitenkin

kin selkeänä, että kansallisen turvallisuuden takaamiseksi tarvitaan ensinnäkin siviilitiedustelun järjestämiseksi sisäministeriöjohtoinen lakivalmistelu, ja toiseksi sotilastiedustelun järjestämiseksi puolustusministeriöjohtoinen lakivalmistelu, sekä molempia hallinnonaloja koskettava sääntely tietoliikenne-tiedustelusta. (Puolustusministeriö, 2015, s. 80–81)

Kyseisessä mietinnössä asian selvimmän ilmaisee liikenne- ja viestintäministeriön nimissä tehty eriävä mielipide työryhmän mietintöön (joka samalla oli ainoa eriävä mielipide ryhmän pysyviltä jäseniltä), joka on liitteenä mietinnön lopussa. Liikenne- ja viestintäministeriö ei kiistä sitä, etteikö puolustusvoimien tiedustelukyvyn kehittäminen olisi tärkeää, tai poliisin tiedonhankintavaltuuksien uudelleentarkastelu olisi perusteltua, vaan kritiikki kohdistuu juuri kyberkeskeisyyteen. Kritiikkiä esitetään perustelulla, että vaikka sotilastiedustelutoiminnasta ei edes säädetä laissa, on silti työryhmä asetettu keskittymään kybertoimintaympäristöön eikä tiedusteluun kokonaisvaltaisesti. Kritiikin ydin on liikenne- ja viestintäministeriöllä siinä, että yleislainsäädäntö tulisi säätää ennen erityislainsäädäntöä; valmistelevan työryhmän toiminnan päätyttyä, jatkotyö pitäisi tämän lausunnon mukaan keskittyä kokonaisvaltaisesti tiedustelulainsäädännön valmisteluun, ei pelkästään tietoverkkotiedustelun toimivaltuuksiin. (Puolustusministeriö, 2015, s. 111)

Mietinnön mukaisesti, vielä samana vuonna 2015, asetettiin hallituksen päätöksellä lainsäädäntötyöhön keskittyvät työryhmät. Sisäministeriö asetti siviilitiedustelulainsäädäntötyöhön syventyvän työryhmän lokakuussa 2015, ja vastaavasti puolustusministeriö asetti samana ajankohtana työryhmän valmistelemaan sotilastiedustelulainsäädäntöä (Sisäministeriö, 2017, s. 8; Nordström ym., 2017, s. 12). Kolmas samaan aikaan, ja samalla mandaatilla, perustettu työryhmä tapahtui oikeusministeriön toimesta. Sen työryhmän tehtävänä oli tarkastella perustuslain muuttamisen tarvetta osana tiedustelulakien säätämistä (kaikkien kolmen työryhmän perustamisen osalta ks. esim. sisäministeriön asiantuntijalausunto 6.10.2015, O 32/2015 vp). Työryhmien työskentely näyttää varsin tarkasti yhteensovitulta ja koordinoidulta, koska esimerkiksi työryhmien Eduskunnan eri valiokunnille antamia asiantuntijalausuntoja vertaillen voi huomata niiden tapahtuneen ajallisesti täysin synkronoituna. Lisäksi valiokunnat käsittelivät eri työryhmien tuotoksia yhden ja saman valtiopäiväasiakirjan alla (asiaa käsiteltiin eri valiokunnissa muun muassa diaarinumeroilla O 32/2015 vp, O 43/2015 vp ja O 32/2016 vp).

Työryhmät saivat työnsä valmiiksi vuoden 2017 keväällä, ja kuten edellisetkin valmistelutyöryhmät, myös nämä julkaisivat loppumietintönsä (Nordström ym., 2017; Sisäministeriö, 2017). Näissä mietinnöissä ehdotettiin luotavaksi kokonaisvaltainen tiedustelulainsäädäntö pelkän tietoverkkotiedustelulain sijaan. Nämä mietinnöt olivat merkittävästi laajempia kuin edellisten työryhmien mietinnöt, jo pelkästään sivumäärällä laskettuna, sekä myös enemmän yksityiskohtiin menevämpiä; mietintöihin oli muun muassa sisällytetty teksti- ja sanamuototarkkuudella uudet lakiehdotukset. Koska tiedustelun yleislaki oli jo pitkälle viety ja tarkka luonnos, oli seuraava jatkotyö enää yhteensovittaa se perustuslain kanssa, ennen kuin hallitus veisi lakiesitykset eduskunnan täysis-

tuntoon. Näin jo aiemmin, vuoden 2015 lopulla työnsä aloittaneen perustuslain tarkasteluun keskittyneen (kyseessä on sama oikeusministeriön asettama työryhmä, josta on maininta aiempana tässä luvussa) työryhmän perusteita tarkistettiin: ryhmän jäsenkoonpano päivitettiin ja uudeksi toimikaudeksi määrättiin ajanjakso loppukevästä 2017 aina kyseisen vuoden loppuun asti. Tehtävänanto ryhmälle säilyi ennallaan, eli tiedustelulainsäädännön ja perustuslain mahdollisten ristiriitojen purkamisen. Nyt vain lakiluonnos tiedustelusta koskevasta lainsäädännöstä tarkentui. (HE 198/2017, s. 4; Sisäministeriö, 2017b)

Käytännössä välittömästi tämän perustuslakikysymyksiä käsittelevän työn päätyttyä hallitus antoi eduskunnalle esityksensä siviili- sekä sotilastiedustelulaeista. Tämä hallituksen esitys annettiin tammikuussa 2018, josta se eteni eduskunnan täysistuntoon helmikuussa 2018. Sieltä lakiesitykset lähetettiin lausuttavaksi lukuisiin eri eduskunnan valiokuntiin. Tästä alkoi loppuvuoden, sekä myös vuodelle 2019 asti kestänyt valiokuntien antamien mietintöjen julkaisusuma. Ensimmäinen aalto valiokuntamietintöjen julkaisemisesta alkoi huhtikuusta 2018 päättyen saman vuoden syksyyn, ja sen jälkeen enää perustuslaki-, puolustus- sekä hallintovaliokunta jatkoi asian parissa työskentelyä muotoillen lakitekstiä hyväksyttävään muotoon. Käytännössä 'hyväksyttävä muoto' tarkoitti sitä, että enää tiedustelulakien perusolemusta tai tarvetta ei kyseenalaistettu (pois lukien pieni vähemmistö, ja toki moniääninen keskustelu kuuluu viisaaseen ja huolelliseen demokraattiseen prosessiin; kommentteista ks. esim. Sisäministeriö, 2017c), vaan kyse oli lakitekstimuotoilusta muun muassa tiedustelun valvonnan, tiedustelusta ilmoittamisen, tiedustelun käytön edellytyksistä eli niin sanotusta välttämättömyysperiaatteesta sekä suhteellisuusperiaatteen eli tiedustelun toimenpiteiden perusteltavuus suhteessa hankittavan tiedon tarkeyteen (PuVM 9/2018, s. 29–65; HaVM 30/2018, s. 92–100).

Tähän lakityöhön liittyi myös syksyllä 2018 eduskunnan päättämä kiireellinen perustuslakimuutos, jonka jälkeen viimeiset valiokuntamietinnöt voitiin luovuttaa eduskunnalle vuoden 2019 maaliskuussa. Tässä kohti on hyvä ymmärtää, että yksityiskohtainen työskentely valiokuntien ja eduskunnan välillä oli monimutkaisempaa, esimerkiksi helmikuussa 2019 eduskunta palautti molemmat lakiesitykset takaisin valiokuntiinsa (siis valmisteluvastuussa oleviin valiokuntiin, eli hallintovaliokunta siviilitiedustelulain osalta ja puolustusvaliokunta sotilastiedustelulain osalta) perustuslakiongelmien vuoksi, jonka jälkeen kyseiset valiokunnat tarvitsivat uudet lausunnot perustuslakivaliokunnalta. Tämä yksityiskohtainen prosessikuvaus ei tässä yhteydessä ole kuitenkaan relevanttia, mutta on hyvä ymmärtää, että ajanjakso vuoden 2018 kevästä vuoden 2019 ei ollut joutokäyntiä tiedustelulakien voimaan saattamisen suhteen. (Eduskunta, 2019; HE 202/2017 sekä HE 203/2017 asioiden käsittelytiedot)

Näin viimeisten muotoilujen ja lakiristiriitojen poistamisen jälkeen hallituksen esitykset siviili- ja sotilastiedustelulaeista etenivät eduskunnan käsitteilyyn maaliskuussa 2019, jolloin ne tulivat myös hyväksytyksi. Yksittäisen lain tarkkuudella sotilastiedustelusta säättää nyt *laki sotilastiedustelusta* (590/2019), ja siviilitiedustelusta pääasiassa *poliisilain* (872/2011) luku 5 a sekä *laki tietoliikennetiedustelusta siviilitiedustelussa* (582/2019), (myös muutamia muita lakeja tai

lainkohtia katsotaan kuuluvan 'tiedustelulait' -kattotermin alle, ks. luku 2.3). Vaikka siviili- ja sotilastiedustelusta säädetään omissa laeissa, on kaikkiin näihin kolmeen lakiin kirjattu tiedusteluviranomaisille velvollisuus toteuttaa yhteistyötä tehtävien tarkoituksenmukaiseksi hoitamiseksi, ja että tietoliikennetiedustelun teknisenä toteuttajana toimii Puolustusvoimien tiedustelulaitos – oli kyseessä sitten siviili- tai sotilastiedustelutehtävä. Ja viimeisenä, eduskunta jätti edellytyksen siitä, että sotilastiedustelulain suhteen puolustusministeriö antaa selvityksen lain toimivuudesta vuoden 2020 loppuun mennessä, ja siviilitiedustelulain suhteen edellytykset siitä, että hallitus seuraa tarkasti siviilitiedustelun tuloksellisuutta, toimivuutta, sekä raportoivan tästä tekemästään seurannasta, sekä edelleen laativan vuoden 2021 loppuun mennessä laajan selonteon siviilitiedustelulainsäädännön tuloksellisuudesta ja toimivuudesta (Eduskunnan vastaukset EV 290/2018 sekä 291/2018). Tasavallan presidentti vahvisti lait huhtikuussa, ja ne astuivat voimaan kesäkuun 1. päivänä vuonna 2019.

2.2.2 Tiedustelulakien tuomat toimivaltuusmuutokset

Sotilastiedustelulain tavoitteena on parantaa Puolustusvoimien tiedonhankintaa sille annettujen tehtävien täyttämiseen liittyen (HE 203/2017, s. 1). Yhteiskunnalle näkyvimmän tehtävän, Suomen sotilaallisen maanpuolustuksen järjestämisen yleiseen asevelvollisuuteen perustuen, lisäksi tehtäväkirjo ulottuu muun muassa maa- ja merialueiden sekä ilmatilan valvontaan, valtionjohdon toiminnanvapauden turvaamiseen, sotilasstrategisen tilannekuvan muodostamiseen ja Suomen turvallisuusympäristön seurantaan (laki Puolustusvoimista 551/2007, HE 264/2006 vp). Näiden tehtävien hoitaminen on määrätty Puolustusvoimia koskevassa laissa (551/2007), ja saman lain yksityiskohtaisissa perusteluissa ohjataan Puolustusvoimien toimintaa vielä siten, että sen tulee tiedustelu- ja valvontajärjestelmällään seurata Suomen turvallisuusympäristöä, tuottaa tietoa vallitsevasta tilanteesta, sekä tuottaa tarvittaessa sotilaallinen ennakkovaroitus (HE 264/2006, s. 17–18). Näin laissa ei määrätä pelkästään Puolustusvoimien tehtävistä, vaan myös tarkemmista menetelmistä, miten kyseiset tehtävät tulee täyttää, ja nämä lait tehtävineen olivat siis jo voimassa ennen tiedustelulakien voimaantuloa.

Näistä tehtävänäannoista huolimatta ennen kesäkuuta 2019, jolloin tiedustelulait tulivat voimaan, sotilastiedustelun toimivaltuuksista ei ollut laissa säädetty (HE 203/2017, s. 12). Ainoastaan sotilasvastatiedustelusta, eli maanpuolustusta vaarantavan (Suomen lakien mukaan) rikollisen toiminnan ennalta estäminen ja paljastaminen Suomen valtion alueella, oli säädetty laissa (laki sotilaskurinpidoista ja rikostorjunnasta puolustusvoimissa 255/2014). Avainsanat tässä yhteydessä ovat rikosperusteisuus sekä Suomen alue. Ensinnäkin poliisilaissa (872/2011) määritellään mitä 'rikosten estäminen ja paljastaminen' toimintana tarkoittaa, sekä mitä salaisia tiedonhankintakeinoja tähän toimintaan liittyen voi toimivaltainen viranomaiskäyttää. Puolustusvoimilla oli käytössä vastatiedustelun toteuttamiseen salaisten tiedonhankintakeinojen osalta rajattu osa poliisin toimivaltuuksista. Puolustusvoimille sallittuja keinoja olivat:

tukiasematietojen, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta sekä viimeisenä kokonaisuutena tekninen kuuntelu, katselu sekä seuranta. Ja puolustusvoimilta ulos rajatut toimet olivat telekuuntelu ja -valvonta (vaikka se olisi perustunut telepäätelaitteen haltijan suostumukseen), valeosto, peitetoiminta ja tietolähde-toiminta, sekä valvottu läpilasku (HE 203/2017, s. 14, 21; poliisilaki 872/2011, 5 luku 1 §). Laissa sotilaskurinpidoista ja rikostorjunnasta puolustusvoimissa kyllä mahdollistettiin poliisiviranomaisen antama apu niissä kohdin, kun Puolustusvoimien rikostorjuntaa toteuttavalla taholla ei ollut riittävää toimivaltaa tarpeellisten tehtäviensä suorittamiseen (255/2014, 90 §; HE 203/2017, s. 15). Käytännössä se tarkoitti sellaisen salaisen tiedonhankintakeinon käyttämistä, mihin poliisilla oli toimivaltuus, mutta sotilasvastatiedustelulla ei.

Puolustusvoimien sotilastiedustelu oli siis järjestetty valtaosin Puolustusvoimien sisäisin ohjein ja määräyksiin (Nordström ym., 2015, s. 32). Lainsäädäntö – tai pikemminkin säättämättömyys – mahdollisti avointen lähteiden tiedustelun, radiosignaalitiedustelun, kuvaustiedustelun sekä rajoitetusti henkilötiedustelun (HE 203/2017, s. 20). Näistä keinoista ensimmäinen, avointen lähteiden tiedustelu, siis julkisesti saatavilla olevaan materiaaliin kohdistuva tiedustelutoiminta, ei edellytä erikseen säädettyä viranomaistoimivaltuutta. Toisena mainittu radiosignaalitiedustelun toteuttaminen järjestettiin Puolustusvoimien sisäisillä ohjeilla, kuten tiedonhankintasuunnitelmilla, ja se kohdistettiin ulkomaisiin kohteisiin, jotka ovat joko kyseisen kohdevaltion sisällä, kansainvälisellä alueella tai kolmannen valtion alueella. Vain tiedustelutehtävien poikkeustapauksissa, kuten alueloukkauksissa, radiosignaalitiedustelua kohdistettiin Suomen alueen sisälle, jolloin tiedustelun kohteena oli kuitenkin edelleen ulkomainen kohde. Luottamukselliseen viestintään radiosignaalitiedustelua ei saa kohdistaa (Puolustusministeriö, 2019, s. 5) Kolmantena mainittu kuvaustiedustelu oli myös järjestetty viraston sisäisillä ohjeilla, kyseisen tiedustelumenetelmän tarkoittaessa elektro-optisten sensorien sekä tutkakuvauksen keinoin hankittavaa tietoa. Esimerkiksi Open Skies -sopimuksen mukaiset kuvauslennot sijoittuvat tähän kategoriaan (ks. esim. Torstila 2020). Nämä tiedustelumenetelmät, avointen lähteiden tiedustelu, kuvaus- ja radiosignaalitiedustelu ovat mahdollista toteuttaa Puolustusvoimien sisäisin määräyksiin siksi, koska näillä tiedonhankintamenetelmillä ei käyttöperiaatteidensa mukaisesti loukata yksityisyyden suojaa tai luottamuksellisen viestin suojaa (HE 203/2017, s. 89). Ja viimeisenä, henkilötiedustelua voidaan, kuten jo mainittua, käyttää rajoitetusti osana Puolustusvoimien rikostorjuntaa, sekä myös kansainvälisessä toiminnassa. Ulkomaisessa toiminnassa mandaatti voi tulla Wienin yleissopimuksen 3. ja 7. artiklasta, jotka viittaavat laillisiin keinoin tapahtuvaan tiedonhankintaan diplomaattistatuksella toimivan sotilasasiainverkoston toimin. Ja toisena mahdollisena käyttötapauksena on kriisinhallintaoperaatioissa tehty henkilötiedustelu, jossa toiminnan legitimointi perustuu kunkin operaation kansainvälisöikeudelliseen mandaattiin, lähettäjämään kansalliseen lainsäädäntöön sekä operaation sisällä annettuihin sotilaskäskyihin. (HE 203/2017, s. 33–35)

Yhteenvedona Puolustusvoimien tiedustelutoimivaltuuksien tilanteesta ennen tiedustelulakeja: Puolustusvoimien salaiset tiedonhankintakeinot perustuivat lakiin sotilaskurinpidoista ja rikostorjunnasta puolustusvoimissa (255/2014), ja yksittäiset salaiset tiedonhankintamenetelmät perustuivat poliisilakiin (872/2011), josta käytössä oli osa poliisin salaisista tiedonhankintatoimivaltuuksista. Näitä salaisia tiedonhankintakeinoja pystyi käyttämään rikosperusteisesti, ja käytännössä siis vastatiedustelutehtävissä. Sotilastiedustelua ei ollut säädetty lailla, vaan toiminta perustui Puolustusvoimien sisäisiin ohjeisiin ja määräyksiin, tai kansainväliseen yhteistyöhön sekä kansainvälisoikeudellisiin lakeihin. Niiltä pieniltä osin mitä tiedustelutoimivaltuuksista säädettiin laissa, eli käytännössä rikostorjunnalliset mandaatit, toimivaltuudet tulivat samoista lainkohdista sotilas- ja siviilitiedustelun kesken; toisin sanon tiedustelutoimivallan jaosta siviili- ja sotilaspuolen kesken ei ollut säädetty missään laissa (HE 202/2017, s. 68).

Tiedustelulakien voimaan tultua sotilastiedustelusta säädetään omassa laissa, joka sisältää säännökset sotilastiedustelun organisoinnista, toimivaltuuksista, ohjauksesta ja seurannasta sekä tiedustelun sisäisestä valvonnasta (HE 203/2017, s. 131). Nyt sotilastiedustelulle luotiin selkeät tehtävät jo lainsäädännössä, kun sotilastiedustelun tarkoitukseksi kirjattiin tiedonhankkiminen ja -käsittely Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta, sekä ylimmän valtionjohdon päätöksenteon tukeminen tiedustelutiedolla (laki sotilastiedustelusta 590/2019, 3 §). Myös muutamia muita tehtäviä nimettiin, jotka ovat tiedustelutiedolla Puolustusvoimien toiminnan tukeminen Suomen maantieteellisen alueen valvomisessa sekä koskemattomuuden turvaamisessa, osallistumisessa kansainväliseen sotilaalliseen kriisinhallintaan tai Euroopan unionin keskinäiseen avunantoon tai aluevalvontaan, taikka muuhun kansainväliseen yhteistyöhön. Myös Puolustusvoimien tehtävien tukeminen kansan elinmahdollisuuksien sekä perusoikeuksien toteutumisen sekä valtionjohdon toiminnanvapauden turvaamisessa nimettiin sotilastiedustelun tehtäväksi. Näin sotilastiedustelulle oli määritelty se viitekehys, mitä varten tiedustelutietoa se saa hankkia.

Myös sotilastiedustelun lailliset kohteet määritettiin, jotka ovat: vieraan valtion asevoimien sekä niihin rinnastettavien järjestäytyneiden joukkojen toiminta, Suomen maanpuolustukseen kohdistuva tiedustelutoiminta, joukkotuhoseisiin liittyvät toiminnot, vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen, kansainvälistä rauhaa uhkaava kriisi, sekä kansainvälistä toimintaa (kriisinhallintaoperaatiot sekä Suomen kansainvälisen avun antaminen) uhkaava toiminta. Ja lisäksi kaikkien näiden kohteiden toiminnan luonne tuli olla sotilaallista, jotta ne ovat kelpoisia sotilastiedustelun kohteita. Ja viimeisenä, sotilastiedustelun kohteena voi olla myös vieraan valtion toiminta, jos se uhkaa Suomen maanpuolustusta tai yhteiskuntamme elintärkeitä toimintoja. (Laki sotilastiedustelusta 590/2019, 4 §)

Edelleen sotilastiedustelulaissa määritetään varsin pitkä listaus sallittuja tiedustelumenetelmiä. Tiivistettynä, nyt sotilastiedustelu voi edelliskappaleissa mainittuihin tarkoituksiin hankkia tiedustelutietoa mainituista kohteista seu-

raavin menetelmin: tarkkailu, peitetty tiedonhankinta (henkilötiedustelu), tekninen tarkkailu, televerkoissa tapahtuva tiedustelu, valeosto, paikkatiedustelu, jäljentäminen, ulkomaan tietojärjestelmätiedustelu sekä tietoliikennetiedustelu. Myös jo ennen tiedustelulakeja käytössä olleet menetelmät, eli avointen lähteiden tiedustelu, kuvaus- sekä radiosignaalityiedustelu, olivat luonnollisesti edelleen käytettävissä; radiosignaalityiedustelu nousi nyt menetelmänä lakitekstiin asti (laki sotilastiedustelusta 590/2019, 60–61 §). Lisäksi kun henkilötiedustelu oli ennen tiedustelulakeja rajattu vain ulkomailla tapahtuvaksi tiedonhankintakeinoksi esimerkiksi osana kriisinhallintaoperaatioita tai diplomaattisen mandaatin alla, nyt henkilötiedustelua pystyy toteuttamaan ilman tällaista valtiokohtaista rajausta, kun laki mahdollistaa 'peitetyn tiedonhankinnan tiedustelutehtävän suorittamiseksi' sekä suunnilleen samoilla kirjausmuodoilla tietolähdetoiminnan (laki sotilastiedustelusta 590/2019, 43 ja 51 §).

Ylipäätään sotilastiedustelutoiminnan ehdot ulkomailla on nyt lakiin kirjattu, ja sotilastiedustelua voi toteuttaa ulkomailla sekä kansainvälisessä yhteistyössä, mikäli se on kansallisten etujemme mukaista. Reunaehdoksi on kielletty osallistumasta ja toteuttamasta sellaista tiedustelutoimintaa, minkä perusteella olisi syytä olettaa, että tietoja luovuttanutta tai yhteistyötä tehnyttä henkilöä uhkaa kuolemanrangaistus, kidutus tai muu ihmisarvoa loukkaava kohtelu (laki sotilastiedustelusta 590/2019, 20 §). Myös ulkomailla sijaitsevaan tietojärjestelmään saa kohdistaa tietoteknisin menetelmin tapahtuvaa tiedustelua, ja edelleen myös tietoliikennetiedustelua saa toteuttaa siinäkin tapauksessa, että tietoliikennetiedustelu on kohdennettu sellaiseen viestintäverkon osaan, jossa tietoliikenne on valtiomme rajat ylittävää (laki sotilastiedustelusta 590/2019, 62 ja 65–68 §). Itse asiassa tietoliikennetiedustelun kohdentaminen sellaiseen viestintään, jossa sekä lähettäjä että vastaanottaja sijaitsevat Suomessa, on kielletty (laki sotilastiedustelusta 590/2019, 82 §) Mutta täytyy muistaa, että näissä teknisissä tiedustelumenetelmissä, kuten kaikissa muissakin tiedustelumenetelmissä, täytyy tarveperustaisuuden vaatimus täytyä.

Yhteenvetona sotilastiedustelulain mukana tuomat muutokset ovat yhtäältä iso nippu teknisen tason toimivaltuusmuutoksia, mutta kaikkia näitä yksityiskohtaisia muutoksia läpileikkaavana elementtinä on ajattelutavan muutos sotilastiedustelun suhteen – ja sama muutos näkyy myös seuraavaksi esiteltävässä siviilitiedustelussa. Kuten sotilastiedustelulakityöryhmä asian ilmaisee, sotilastiedustelu ei ole samalla tavalla henkilö- ja rikossidonnaista kuin rikosten ennalta estäminen, vaan yhtenä keskeisimpänä tarkoituksena on tuottaa mahdollisimman reaaliaikaista tietoa turvallisuusympäristömme kehityksestä (HE 203/2017, s. 135). Tämä ajattelutavan muutos ilmenee siinä, että sotilastiedustelua ei enää tarvitse suorittaa puutteellisin tai sääntelemättömin toimivaltuuksin, ja osin pelkästään rikosepäilyperusteisin toimivaltuuksin.

Kansallisen tiedustelutoiminnan siviiliviranomaispuolella tilanne oli josain määrin sama, eli laeissa ei tiedustelun toimivaltuuksista ollut säädetty ennen nykymuotoisia tiedustelulakeja. Eli, ensinnäkin kansallisesta turvallisuudesta vastaavien siviiliviranomaisten tehtävänä on ennakoivasti hankkia tietoja sellaisista toiminnoista ja hankkeista, joka voi vaarantaa tai uhata kansallisia

etuja tai turvallisuutta. Suomessa tällaista viranomais toimintaa toteuttaa Suojelupoliisi, jonka sanotarkaksi tehtäväksi oli muotoiltu ”torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa” (Laki poliisin hallinnosta 110/1992 10 §, jonka pykälän sanamuodot otettu lainaukseen aiemmasta ajantasamuodosta 10.7.2015/860, koska tiedustelulakien yhteydessä myös tätä lakia päivitettiin). Sen kummemmin itse lakitekstissä kuin sen esitöissä (esim. HE 364/2014) ei määritellä tarkemmin *hankkeen* käsitettä, mutta lakiteksti antaa selvästi ymmärtää, että hankkeissa ei katsota kyse olevan rikoksista. Tältä osin Suojelupoliisin kohdistuu vaatimus toteuttaa tiedustelullista toimintaa rikostorjunnallisen toiminnan ohessa. (HE 202/2017, s. 68)

Näiden tehtävien suorittamiseksi Suojelupoliisilla oli tällöin, ennen tiedustelulakeja, samat esitutkinta- ja pakkokeino toimivaltuudet kuin muillakin poliisiviranomaisilla. Suojelupoliisin toimivaltuudet perustuivat yleisiin poliisin toimivaltuuksiin, sellaisin sanamuodoin kuten poliisilaissa säädettiin. Esimerkiksi salaiset tiedonhankintakeinot olivat poliisilain 5. luvun mukaiset, tosin ilman niitä rajoituksia, joita sotilasvastatiedustelulle asetettiin (kuten tässä luvussa aiemmin kerrottiin).

Kuitenkaan sen hetken lakisääntelyssä toimivaltuuksien osalta – äskeinen lakilainaus oli siis niin sanotusti tehtävänanto – ei ollut otettu huomioon kuin rikostorjuntaan perustuvat tiedonhankintatoimivaltuudet (HE 202/2017, s. 68). Suojelupoliisi toimi myös esitutkintaviranomaisena, eli se suoritti edelliskappaleessa mainitun lainauksen sisällä kuvattujen rikosten tai rikosepäilyjen tutkintaa. Käytännössä Suojelupoliisin salainen tiedonhankintatoiminta oli lainsäädännön myötä mahdollista kohdistaa, ja sitä sai toteuttaa, vain sellaisiin kohteisiin, jotka sijaitsivat Suomessa, olivat yksilöitävissä olevia henkilöitä, ja jotka tietyllä todennäköisyydellä olivat syylistyneet, tai syylistymässä, rikokseen (Sisäministeriö, 2019b). Myös jo tapahtuneiden rikosten selvittäminen toi mandaatin Suojelupoliisin salaiselle tiedonhankinnalle, kunhan vain kohde sijaitsi Suomen rajojen sisällä ja oli yksilöitävissä oleva (Aaltomaa, 2017).

Koska Suojelupoliisin tehtävä edellytti käytännössä tiedonhankintaa myös Suomen rajojen ulkopuolelta, on syytä korostaa se seikka, että rikosperusteinen toimivaltuus oli voimassa luonnollisesti vain Suomen valtion alueella – juuri samoin kuin sotilasvastatiedustelunkin rikosperusteiset toimivaltuudet. Ulkomaita koskeva tiedonhankinta nojasi siis käytännössä Suojelupoliisin harjoittamaan kansainväliseen tiedusteluyhteistyöhön, avointen lähteiden tiedusteluun sekä Suojelupoliisin omaan yhteyshenkilötoimintaan (Nordström ym., 2015, s. 31).

Koska ennen tiedustelulakeja Suojelupoliisi toimiakseen nojautui siis poliisin niin sanottuihin yleislakeihin ja käytti poliisiviranomaisen toimivaltaa, oli luonnollista, että poliisitoimi ohjasi Suojelupoliisin toimintaa. Ajallisesti tiedustelulakien luomisen ja voimaan saattamisen yhteydessä tapahtui myös Suojelupoliisin organisaatorakennemuutos, jossa Suojelupoliisi hallinnollisesti siirrettiin sisäministeriön poliisitoimesta itsenäisen, sisäisen turvallisuuden yksikön alle. Tämä prosessi on tarkemmin kuvattu luvussa 2.1, ja tässä kohtaa

tämä tiedustelulakien lomassa mennyt muutos on vain mainintana, jotta lukija ymmärtää kokonaiskuvan ja osaa yhdistää nämä kaksi tapahtumaa yhdeksi kokonaisuudeksi.

Tiedustelulakien säätämisen jälkeen siviilitiedustelulainsäädännön kehys on jaettu kahteen osaan, jossa henkilö- ja tietojärjestelmätiedustelusta säädetään poliislakiin uudessa 5 a luvussa, ja tietoliikennetiedustelusta säädetään omassa laissa tietoliikennetiedustelusta siviilitiedustelussa. Peruste tähän jakolinjaan oli se, että tietoliikennetiedustelussa nähtiin niin paljon vain kyseiselle tiedonhankintamenetelmälle ominaisia piirteitä, jotta siitä kannattaa säätää omassa laissaan (HE 202/2017, s. 109). Sallitut ja käytössä olevan tiedustelumenetelmät pohjautuvat pääosin aiemman poliisilain 5 luvussa esitelyjen salaisten tiedonhankintamenetelmien mukaisesti. Uusina tiedustelumenetelminä tiedonhankinnan keinovalikomaan tuli paikkatiedustelu, jäljentäminen, lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten, ja viimeisenä tietoliikennetiedustelu – josta on siis, kuten mainittua, oma lakinsa. (Sisäministeriö, 2019b, s. 5).

Nyt näiden lakien mukaisia, mainittuja tiedustelumenetelmiä pystyi Suojelupoliisi käyttämään tiedonhankinnassa aina kun tarkoituksena on kansallisen turvallisuuden suojaaminen, ylimmän valtiojohdon päätöksenteon tukeminen tai muiden viranomaisten tukeminen heidän hoitaessaan lakisääteisiään kansallisen turvallisuuden tehtäviä (HE 202/2017, s. 114). Myös siviilitiedustelun kohteista määrätään laissa erikseen, eli Suojelupoliisi voi toteuttaa tiedonhankintaa määrättyjä tarkoituksiaan varten, kun kohteena on joko: terrorismi, ulkomainen tiedustelutoiminta, joukkotuhoaseet, kaksikäyttötuotteet, yhteiskuntajärjestystä tai yhteiskunnan kriittisiä toimintoja uhkaava toiminta, suuren ihmismäärän henkeä tai terveyttä uhkaava toiminta, vieraan valtion Suomea kohtaan toteuttama uhkaava toiminta, kansainvälistä rauhaa ja turvallisuutta uhkaava toiminta sekä kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta (poliisilaki 872/2011, 5 a luku 3 §). Nähdään siis, että rikosperusteisuus on täysin hävinnyt tiedustelutoiminnan toteuttamisen edellytyksistä.

Samalla kun tiedustelulait tulivat voimaan, antoi sisäministeriö asetuksen, jolla poistettiin Suojelupoliisilta sen esitutkintaviranomaisen asema (Sisäministeriö, 2019c). Tiedustelutiedonhankinnan toteuttaminen ei enää edellyttänyt rikosperusteisuutta, mutta mikäli tiedustelun aikana ilmeni syytä epäillä rikosta, voitiin tietyin edellytyksin jatkaa tiedustelun toteuttamista rikostutkintaa varten, sekä hankittu aineisto voitiin luovuttaa rikostutkintaa suorittavalle viranomaiselle (poliisilaki 872/2011, 5 a luku 4 §; Pöysti, 2021, s. 7). Myös poliisin hallinnosta annetussa laissa (110/1992, 10 §) muutettiin Suojelupoliisin tehtävässä sanamuoto *”torjua sellaisia hankkeita ja rikoksia...”* muotoon *”hankkia tietoa kansallisen turvallisuuden suojaamiseksi...”*.

Ja viimeisenä, siviilitiedustelun osalta laadittiin siis oma laki koskien tietoliikennetiedustelua (582/2019), kun sotilastiedustelussa se upotettiin saman sotilastiedustelulain (590/2019) sisään. Tietoliikennetiedustelun kohteet ovat yhtäläiset kuin muussakin siviilitiedustelussa, ja muutkin tiedustelutoiminnan

periaatteet, kuten suhteellisuusperiaate, tarkoitussidonnaisuus sekä vähimmän haitan periaate, pätevät yhtä lailla tietoliikennetiedusteluun (laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019, 1 §). Tietoliikennetiedustelu - niin sotilas- kuin siviilitiedustelussa - ei saa olla yleistä ja kohdentamatonta tietoliikenteen seurantaan, vaan sen tulee perustua ensimmäisessä vaiheessa automatisoidulla erottelulla perustuvaan tekniseen tiedonhankintaan. Esimerkiksi tiettyjä hakuparametreja asettamalla voidaan luoda automaattisia haku- ja suodatus-toimintoja. Nämä hakuehdot eivät saa kohdistua seurattavan tietoliikenteen sisällä olevien viestien sisältöihin, vaan ne voi kohdistaa viestien tunnistetta- ja metatietoihin. Vain tietyissä, harvoissa erikoistapauksissa hakuehto voi kohdistua viestin sisältöön. Jatkokäsittelyä voidaan laillisesti tehdä myös manuaalisesti, tai toteuttaa lisäsuodatusta seuraavin automaattisin suodatusparametrein. Näin tietoliikennetiedustelu jakaa samat yleiset periaatteet muidenkin tiedustelumenetelmien kanssa, asemoituen siis yhdeksi tiedonhankintamenetelmäksi muiden menetelmien joukkoon. (Laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019, 4-6, 12 §)

Seuraavaksi esitellään esimerkkejä tiedustelutoiminnan sääntelystä eri Euroopan valtioista, kun kotimainen sääntely ja toimivaltuudet ovat nyt tulleet esitellyiksi. Yksityiskohtaisuudessa ei pureuduta samalle tasolle asti kuin tässä nyt päättyvässä kotimaisen tiedustelukentän tarkastelussa, vaan muiden maiden tapausesimerkeillä pyritään luomaan lukijalle kuvaa eurooppalaisen tiedustelutoiminnan sääntelystä yleisemmin. Tällöin voidaan esimerkiksi tehdä vertailua kotimaisten ja ulkomaisen tiedustelutoiminnan järjestämisen välillä.

2.3 Tiedustelutoiminnan sääntely muissa maissa - tapausesimerkkejä

Tämän tutkimusaiheen keskeinen ongelma ei suinkaan ole vain suomalaissa yhteiskunnassa esiintyvä, vaan kansallisen tiedustelun tiedonhankinnan laajuuden sekä yksilönvapauden ja -suojan välinen tasapaino on dilemma yleisesti länsimaisessa yhteiskuntakulttuurissa (ks. esim. Martin, 2004; Cole & Dempsey, 2006; Deflem & McDonough, 2015). Myös muun muassa Eduskunnan kirjasto on koonnut tiedustelulakien valmisteluvaiheessa tähän problematiikkaan liittyvää kirjallisuutta ja tutkimusaineistoa (Eduskunta, 2019), ja tähän ongelmaan palataan vielä tämän luvun lopussa. Muiden länsimaiden tiedustelulainsäädäntöä on analysoitu kotimaisten tiedustelulakien valmisteluvaiheessa, kun esimerkiksi puolustusministeriön mietinnössä sotilastiedustelulaeista eritellään Ruotsin, Norjan, Tanskan, Saksan, Alankomaiden sekä Sveitsin lakisäätelyä koskien heidän kansallisista tavoista järjestää tiedustelutoiminta (Nordström ym., 2017, s. 77-98).

Myös siviilitiedustelulainsäädännön valmistelussa kansainvälinen vertailu on otettu vastaavalla tavalla huomioon, sillä sisäministeriön (2017) mietintö käsittelee kansainvälisiä näkökulmia. Teksti on tosin monilta osin samaa kuin

puolustusministeriön julkaisussa. Mietinnöissä kerrotaan edelliskappaleessa mainittujen valtioiden tiedustelupalveluiden tehtävät, ja mietintöjen välillä ei ole suuria eroja keskenään, vain sanavalinnat ja tietyt painotukset vaihtelevat. Mikäli näiden kuuden valtion otannan perusteella tehdään valtiollisesta tiedustelupalvelusta yleistys, niin kyseisen instanssin tehtävänä on kartoittaa valtioon kohdistuvia ulkoisia ja sisäisiä uhkia, laatia kansallisia uhka-arvioita sekä tukea ulko-, turvallisuus- ja puolustuspolitiikan tekemistä (Nordström ym., 2017, s. 78, 82, 85, 88, 93, 96). Mielenkiintoisesti Norjan kohdalla korostetaan, että tiedustelupalvelulle käsketty kansallisten etujen turvaamisen tehtävää ei voida muotoilla tyhjentäväksi luetteloksi, koska tällainen luettelo siitä, mitkä ovat turvattavia kansallisia etuja, elää ja muuttuu ajassa (Nordström ym., 2017, s. 82). Tämä toteamus vahvistaa sitä väitettä, joka on tämänkin tutkielman keskeinen teema, eli kansallisten uhkien luonne on muuttuva.

Kun siirrytään tarkastelemaan mietintöjen referointia kyseisten valtioiden tiedustelutoiminnan sääntelystä, tulee esiin merkittävästi isompia valtioiden välisiä eroja. Yhteistä tarkastelujoukon valtioille – siis Ruotsi, Norja, Tanska, Saksa, Alankomaat ja Sveitsi – on se, että tiedustelutoiminnasta säädetään laeilla. Tämä ei ole yllättävää, sillä yleisesti länsimaisessa yhteiskuntarakenteessa säädetään laeilla ja niitä tarkentavilla asetuksilla kaikkien julkista valtaa käyttävien organisaatioiden toiminnasta. Puolustusministeriön (Nordström ym., 2017, s. 77–98) mietinnössä esitettyjen kuvausten perusteella lähimpänä suomalaista tapaa säätää tiedustelutoiminta on Ruotsin malli.

Ruotsin mallissa valtiollisen tiedustelun sääntely koostuu useasta eri laista, tiedustelun toteuttaminen edellyttää tuomioistuimen lupaa, kyseisestä luvasta pitää tulla ilmi määrättyjä yksityiskohtia (kuten tiedonhakutehtävä ja luvan ajallinen kesto). Myös samoja velvollisuuksia on säädetty kuin Suomessa, joita on esimerkiksi tietojen hävittämisvelvollisuus, mikäli tietoliikennetiedustelulla on saatu tietoja, joilla ei ole merkitystä tiedustelutoiminnan kannalta. Velvollisuuksia on myös ilmoittaa tapahtuneesta tiedustelusta tiedustelun kohteelle, ellei erinäiset salassapitomääräykset tätä ilmoitusta estä. (Nordström ym., 2017, s. 79)

Kun nyt on kuvattu yksi tarkastelujoukon tarkimmin säännellyistä valtiollisen tiedustelun toteutustavoista, eli Ruotsin malli, on toisessa laidassa Tanska. Heillä on kaksi tiedustelupalvelua, joista toinen keskittyy ulkomaantiedusteluun sekä sotilastiedusteluun (FE, eng. *Danish Defence Intelligence Service*), ja toinen palvelu on kotimaan turvallisuus- ja tiedustelupalvelu (PET, eng. *Danish Security and Intelligence Service*). Heidän tiedustelupalvelujen toteuttamasta tiedonhankinnasta, tai sen käytön edellytyksistä, ei säädetä laeilla tarkemmin kuin toteamalla yleisesti, ”tiedustelupalvelu voi kerätä ja hankkia sellaista tietoa, jolla voi olla merkitystä tiedustelupalvelun toiminnalle” (LBK nr 1600 af 19/12/2014, luku 2; LBK nr 1287 af 28/11/2017, luku 2. Kyseessä on lait kummankin tiedustelupalvelun toiminnasta). Toki myös velvollisuuksia tiedustelutoiminnalle osoitetaan, kuten vastuuministerien (oikeusministeri kotimaan asioista ja puolustusministeri ulkomaan-

ja sotilasasioista) tietoisena pito ”turvallisuuden kannalta tärkeistä seikoista” (samat lait, luku 1). (Nordström ym., 2017, s. 86)

Tätä suurta eroavaisuutta tarkastellessa ei voi olla ajattelematta tutkielman tekohetken aikoihin mediassa esiin tuotua uutisointia Tanskan tiedustelupalvelujen, lievästi sanottuna, arveluttavasta toiminnasta. Väitetysti Tanskan tiedustelupalvelut olisivat tehneet yhteistyötä Yhdysvaltain tiedustelupalvelujen kanssa hankkimalla Yhdysvaltain edustajille tietoa eurooppalaisista virkamiehistä ja poliitikoista ilman laillista perustetta tiedusteluun, sekä myös sallimalla Yhdysvaltain toteuttaa saman tyyppistä tiedustelua Tanskan kautta. (”Tanskan sotilastiedustelun epäillään vakoilleen tanskalaisia Yhdysvaltain tiedusteluviranomaisten avustamana” Yle 24.9.2020, ”SVT ja DR: Yhdysvallat vakoili ruotsalaisia, norjalaisia, ranskalaisia ja saksalaisia poliitikkoja sekä virkamiehiä Tanskan kautta” Yle 30.5.2021)

Nämä mainitut Tanskan tapahtumat ovat kirvoittaneet niin eurooppalaisia kuin Tanskassa tapahtuvaa keskustelua heidän kansallista tiedusteluansa sääntelevien lakien tiukkuudesta. Elokuussa 2020 Euroopan parlamentista esitettiin kysymys Euroopan komissiolle – siis taholle, joka käyttää EU:n lainsäädäntövaltaa laatimalla esitykset EU:n säädöksistä, valvoo niiden täytäntöönpanoa sekä kansallista soveltamista. Tässä kysymyksessä (kirjallinen kysymys E-004645/2020, 26.8.2020) haluttiin saada selko muun muassa siitä, miten Tanskan skandaalinomaiset tapahtumat vaikuttavat viranomais- ja turvallisuusyhteistyöhön EU:n piirissä, kun kyseinen työ edellyttää keskinäistä luottamusta siitä, että vaihdettavaa tietoa käsitellään asianmukaisesti kaikkien jäsenvaltioiden taholla. Komissiolta pyydettiin vastausta myös siihen, aikooko se organisaationa tutkia tapauksen siitä näkökulmasta, onko EU:n kansalaisten perusoikeuksia rikottu Tanskan tapahtumiin liittyen. Kysymyspatteri päätettiin koko lakisääntelykysymyksen keskeiseen elementtiin, eli miten Euroopan komissio aikoo seuraavassa Euroopan turvallisuusstrategiassa varmistaa kansalaistensa oikeuksien turvaamisen tällaisten mielivaltaisten tiedonhankinta- ja valvontatapausten varalta.

Tanskassa kriittiset kommentit ovat liittyneet juuri tähän samaan tasapainoon, eli ovatko tiedustelulait jo liian sallivia yksityisyydensuojan ja liikesalaisuuksien kustannuksella. Muun muassa muutamat pilvi- ja muita digitaalisia palveluita tarjoavien yritysten johtohahmot ovat ilmaisseet huolensa vuonna 2019 esitettyjen laajojen viranomaisen tiedonsaantivaltuuksien negatiivisen vaikutuksen liiketoimintamahdollisuuksiin (Brun & Pedersen, 2019). Käytännössä negatiivinen vaikutus syntyy kirjoittajien mukaan siitä, että viranomaisella olisi ilman oikeuden päätöstä oikeus saada pyytämäänsä dataa tai tietoa kolmannelta osapuolelta, kuten yksityisomisteiselta organisaatiolta tai yritykseltä. Pääsääntöisesti keskusteluissa kyllä hyväksytään tiedustelu- ja tiedonhankintalakien tarkoitusperä, kansallisen turvallisuuden takaaminen (kuten Suomessakin vallitsi laaja konsensus tiedustelulakien valmisteluvaiheen keskusteluissa, ks. esim. Mannonen, 2020). Tämän periaatteellisen hyväksynnän antavat myös kirjoittajat Brun & Pedersen (2019), mutta ongelmaksi nostetaan se, että nyt – Tanskan tapauksessa – esitetään aivan liian laajoja ja valvomatto-

mia tiedonsaantioikeuksia. Yrityksillä ei ole edellytystä harjoittaa menestyksekkästä liiketoimintaa sellaisen valtion alueella, jossa on jatkuva mahdollisuus, että omat yrityssalaisuuksien piiriin tai muuten sensitiiviset tiedot määrätään luovutettavaksi viranomaiselle.

Brun & Pedersen (2019) kohdistivat helmikuussa 2019 kirjoituksessaan kritiikin siis lakiesitystä kohtaan, ja kirjoituksen keskiössä oli tiedonluovutus viranomaiselle ilman, että tuomioistuimien käsittelisi viranomaisen tiedonhankintatarvetta. Elokuussa 2019 vahvistettiin Tanskassa voimaan laki Kyberturvallisuuskeskuksesta, jonka sisältö oli tiedonsaantioikeuksien osalta muuttumaton kritiikin kohteeksi joutuneesta lakiesityksestä (LBK nr 836 af 07/08/2019; tässä yhteydessä keskeistä on lainkohdat luvusta 4, § 4–6 c).

Tätä moninaista kenttää, missä tiedusteluorganisaatio nykyaikana luovii, on teoretisoitu muun muassa Graaff (2014, s. 1). Hän selittää tiedusteluorganisaation kuuluvat useaan eri ympäristöön. Yksi on hierarkkinen ja virallinen ympäristö, jossa tiedusteluorganisaatio saa muun muassa tehtävänsä. Toinen ympäristö on niin sanottu arvoympäristö, joka on se kulttuurillinen ja ideologinen ympäristö ja yhteiskunta, jossa tiedusteluorganisaatio toimii. Kuten edellä Tanskan esimerkistä nähdään, nämä ympäristöt voivat reaali maailmassa olla kovastikin ristiriitaisessa suhteessa keskenään.

Itse asiassa tämä ristiriitaisuus nähdään laajemminkin nykyajan tiedustelutoiminnan keskeisenä kysymyksenä. Omand & Phythian (2018, s. vii) esittävät peitetyn tiedonhankinnan etiikkaa käsittelevän teoksensa esipuheessa teesinsä, jonka mukaan nykypäivän isoimpia ratkaisemattomia kysymyksiä tiedustelutoiminnassa on se, kuinka pitkälle valtion on hyväksyttävää mennä tiedustelutiedon hankkimisessa sekä saadun tiedon hyödyntämisessä. Ongelma on heidän mukaansa käsinkosketeltavan todellinen juuri 2000-luvun demokraattisissa yhteiskunnissa, joissa erityisessä arvossa pidetään yksityisyyden suojaa ja kansalaisvapauksia. Tanskan tapahtumat toimivat erinomaisena tausesimerkkinä tästä. Mainittakoon myös se, että teoksen tekijöitä voi luonnehtia toimialasta tietäviksi; sir David Omand on toiminut muun muassa Iso-Britannian tiedustelu- ja turvallisuuspalvelu GCHQ:n pääjohtajana.

Samaan aikaan tämän länsimaissa nyt vallalla olevan kansallisoikeuksia ja -vapauksia korostavan demokratiakäsityksen kanssa, on kansallinen turvallisuuskäsite murroksessa. Vielä 1900-luvun loppupuolelle asti kansallinen turvallisuus tai kansalliset uhkakuvat liitettiin niin sanotusti perinteisiin uhkiin, kuten sotilaallisen voimankäytön kohteeksi joutumisen uhkaan. Voiko turvallisuuskäsitteen murros olla yksi selittävä tekijä esimerkiksi sen dilemman taustalla, minkä Omand & Phythian esitti tiedustelun etiikkaan liittyen? Sumentavatko uudet, monitahoisemmat ja abstraktimmat uhkat kansallista turvallisuuskäsitettä sen suhteen, mitä toimia turvallisuuden ylläpito vaatii? Seuraavassa luvussa tarkastellaan kansallisen turvallisuuden murrosta, sekä turvallisuuden ja uhkakuvien välistä suhdetta.

2.4 Turvallisuuskäsitteen suhde kansallisiin uhkakuviin

Tämä luku tarjoaa turvallisuuskäsitteen erittelyn lisäksi sen ja kansallisten uhkakuvien välistä vertailua. Lisäksi tämä luku pohjustaa ja taustoittaa – luo laajempaa viitekehystä – pääluvun 3 ydinsisältöä, joka on hybridiuhkakäsitteen muodostaminen. Tämä hybridiuhkakäsite muodostetaan luvussa 3.3.6, jonka alkukappaleissa sivutaan tiivistetysti myös tässä luvussa laajemmalti esitettyjä asioita.

Viime vuosisadan jälkimmäisellä puoliskolla, kylmän sodan aikana, Suomen turvallisuuskäsitys oli pitkälti kovaan ulkoiseen turvallisuuteen painottunut. Sotilaallinen uhka oli hallitsevassa asemassa kansakunnan uhkakuvissa, vaikka YYA-sopimuksen hengessä Neuvostoliiton muodostamaa hyökkäyksellistä uhkaa ei virallisiin asiakirjoihin tullut lausua, jolloin viralliset uhkakuvat olivat hyvin neutraaleja. Turvallisuuspolitiikka oli pitkälti presidenttijohtoista, ja sitä tehtiin vahvassa symbioosissa puolustuspolitiikan kanssa. Tämän vahvan ohjauksen myötä laaja-alainen ja ennen kaikkea kriittinen yhteiskunnallinen keskustelu oli poissa. Myös muut tekijät saattoivat vaikuttaa keskustelun vähäisyyteen, kuten sotien jälkeinen halu keskittyä normaaliin elämään, ilman jatkuvaa omaa osallistumista sotilaallisten uhkakuvien ruotimiseen. (Limnell & Iloniemi, 2018, s. 60–61)

Uhkakuvien näkökulmasta uusi aikakausi koitti viime vuosisadan lopun tapahtumarykelmän myötä: kylmän sota päättyi, YYA-sopimus raukesi, sekä Suomen liittyi EU-jäseneksi. Sotilaallisia kyvykkyyksiä alettiin Euroopassa purkamaan, tai vähintäänkin rajoittamaan, ja sotilaallisten suorituskykyjen valvontaa parannettiin (Torstila, 2020). Tämä kaikki avarsi Suomessa käytävää niin uhka- kuin turvallisuuskeskustelua (Limnell & Iloniemi, 2018, s. 61). Vuonna 1995 julkaistu ensimmäinen turvallisuuspoliittinen selonteko virallisti laajan turvallisuuskäsitteen (Limnell, 2021). Miksi nämä molemmat, sekä uhka- että turvallisuuskeskustelut avautuivat ja todella käynnistyivät, niin kun käsitellään uhkia, on siinä erottamattomana osana se kohde, jota käsittelyssä olevilta uhkilta halutaan suojata. Uhka on kontekstisidonnainen asia; ei yhteiskunnallisen tason turvallisuustyössä ole relevanttia käsitellä yksilötason uhkia – onko pakkasaamuisella pihallani liukastumisen uhkaa, vai onko ulko-oven edusta jo hiekoitettu. Näin ollen uhkakeskusteluun pitää liittää mukaan kohde, jota halutaan turvata uhkilta. Uhkat ja turvallisuus ovat tiettyssä mielessä saman asian kaksi eri puolta.

Välittömästi tämän 1990-luvulla tapahtuneen tapahtumarykelmän jälkeen, ja osin jo sen aikaan, globalisaatio otti harppauksia eteenpäin vieden maapallon kansallisvaltioita alati syvenevään keskinäisten riippuvuussuhteiden verkkoon. Turvallisuuskäsitys laajeni myös tämän verkottumis -tekijän johdosta. Kun aiemmin uhkat – ja siis samalla turvallisuus – yhteiskunnallisella tasolla koski vahvasti valtion ulkoista turvallisuutta painottuen sotilaallisiin uhkiin, nousi nyt yhteiskunnalliseen keskusteluun myös globaalit uhkat. Globalisoituvan maailman ongelmista, kuten väestönkasvusta ja luonnonvarojen niukkuudesta,

muodostettiin sellaisia uhkakäsityksiä, joihin tuli vastata niin kansallisin kuin kansainvälisin rakentein ja resurssein (Limnell & Itoniemi, 2018, s. 61). Globaalit uhkat tulivat siis osaksi yksittäisen valtion uhkakuvia.

Tänä päivänä länsimaisessa kulttuurissa ja valtioissa termit globalisaatio tai keskinäisriippuvainen maailma ovat jo päivänselviä asioita, ja yhtenä valtiollisen toiminnan perustana pidetään yhteistyötä yli kansallisvaltioiden rajojen. Iso-Britannian vuosikausia kestänyt EU -eroproessi on yksi osoitus tästä; yhdestä kansainvälisestä rakenteesta irrottautuminen ja sen tilalle korvaavien erillissopimusten neuvottelemisen on kaikkea muuta kuin helppo prosessi. Eikä suomalainen yhteiskunta tee poikkeusta globalisoitumisen tason syvyydessä. Ulko- ja turvallisuuspolitiikkamme keskeinen johtotaho on tasavallan presidentti (Ulkoministeriö, 2010, s. 46), ja nykyinen presidentti Sauli Niinistö on useassa eri tapahtumassa linjannut Suomen turvallisuuspolitiikan perustuvan neljälle pilarille (Niinistö, 2018). Näistä pilareista kolme liittyy suoraan kansainväliseen yhteistyöhön. Myös neljäs pilari, eli kansallinen puolustuskyky, tarkoittaa kansainvälistä toimintaa, sillä puolustuskykyä ylläpitää Puolustusvoimat, joka toimii jatkuvassa vuorovaikutuksessa kansainvälisten kumppaneidensa kanssa.

Globalisoitumisen myötä tullutta *laajennettua turvallisuuskäsitystä* voi näin ollen pitää vallitsevana ja todellisena olotilana. Mutta tulisiko 2010-luvulla alkanutta informaation, uutisten, ja digitaalisen viestinnän saatavuuden, ja oikeastaan tiedon digivirtauksen myötä laajentaa yhteiskunnallista turvallisuuskäsitystä edelleen? Vastaus on varmasti helppo sanoa myöntäväksi, mutta miten tätä keskustelua tulisi tehdä hedelmälliseksi ja konkreettiseksi pelkän hyväksyvän ja samanmielisen nyökyttelyn sijaan? Tulee ensinnäkin selvittää lähtökohdat – miten tähän tiedon yltäkylläisyyden pisteeseen on tultu, jonka jälkeen tutkia ilmiötä, ja näiden synteillä voitaisiin tuottaa tietoa siihen päätöksentekoon, jossa muodostetaan kansalliset uhkat, sekä mietitään kuinka niihin kansallisesti vastataan.

Lähtökohdiksi tulee tunnustaa se, että vaikka tietotekniikka on ottanut valtavia kehitysaskelaita jo ennen 2010-lukua, mikäli kehitystä tarkastellaan esimerkiksi Mooren lain mukaisesti tietokonemikropiirien laskentatehon kasvuna. Mutta siitä huolimatta nykyisen kaltainen kommunikaatioteknologian ja -tapojen ilmiö, jossa isoja datamassoja voidaan sirtää globaalisti lähes viiveettömästi, ei ole ollut todellisuutta kuin hädän tuskin vuosikymmenen ajan, alkaen 2010-luvulta. Teknologisessa kehityksessä ei enää pidetäkään niin merkityksellisenä itse laskentatehon kasvua, vaan keskiössä on muun muassa tekoälyn kehittyminen (mm. Huangin laki, ks. esim. Perry, 2018), teknisten laitteiden integroituminen osaksi kaikkia arkipäivän toimintoja, sekä datan määrän ja siirtonopeuksien kasvu (Waldrop, 2016). Seuraavassa alaluvussa jatketaan laajentuneesta turvallisuuskäsitteestä lähemmäksi kohti nykypäivää, ja esitellään kuinka muutamat viranomaiset määrittelevät nykypäivän hybridiuhkakäsitetä. Tässä määrittelyssä voidaan havaita, että ainakin osa viranomaisista tunnistaa informaatiolla vaikuttamisen merkityksen osana nykyaikaisia uhkia. Myös myöhemmin seuraavassa pääluvussa, jossa

varsinainen tutkimusaineiston koodaus tehdään, voidaan havaita, että informaatio- ja kybervaikuttamisella on itse asiassa aika isokin rooli osana nykyaikaisia uhkakuvia.

2.5 Turvallisuusviranomaisten määritelmät hybridiuhkista

Tässä tutkielmassa käytetään kaikissa niissä yhteyksissä, missä ei viitata tutkielmassa muodostettuun kansalliseen hybridiuhkakäsitteeseen (luku 3.3.6), kansallisten turvallisuusviranomaisten määritelmiä hybridiuhkista. Tämä johtuu siitä, että viranomaistoiminta, ja erityisesti turvallisuusviranomaiset ovat muutenkin tutkielman keskiössä. Näin tutkielmaa lukiessa voi peilata turvallisuusviranomaisten määritelmää hybridiuhkista kansalliseen poliittiseen määritelmään, joka tässä pääluvussa myöhemmin muodostetaan. Lienee mielenkiintoista, ja ehkä joitain jatkotutkimuskysymyksiäkin nostattavaa, mikäli eroavaisuuksia on löydettävissä viranomaisten ja poliittisten määritelmien välillä.

Hybridiuhkiin tai -vaikuttamiseen ei ole yhtä, yleisesti hyväksyttyä määritelmää, vaan muun muassa Eduskunnan hallintovaliokunta selittää hybridi -käsitteen muuttuvaa luonnetta seuraavalla tavalla: hybridiuhkien määritelmät vaihtelevat siksi, että käsitteen määrittely on haluttu pitää mahdollisimman joustavana uhkien muuttuvan ja moninaisen luonteen vuoksi, ja hybridiuhka määritellään yleensä kuvaamalla niitä keinoja, joita käytetään hybridivaikuttamisessa (HaVM 30/2018, s. 16). Ja hallintovaliokuntahan sille määrättyjen tehtäviensä mukaisesti antoi mietinnön hallituksen esitykseen siviilitiedustelulaeista, joten valiokunnan näkemyksen voi perustellusti mieltää varsin suuren painoarvon omaavaksi.

Kun siis pääsääntöisesti hybridiuhkia tarkastellaan toiminnan kautta, niin käytännössä tähän käsitteeseen liitetään erottamattomana ja olennaisena osana toiminnan tavoitteellisuus. Siis jokin, yleensä valtiollinen tai ei-valtiollinen, mutta vaikutukseen käytettävien resurssien puolesta siihen rinnastettava (toimijamäärittelystä ks. esim. Tiilikainen, 2020), toimija käyttää monimuotoisia keinoja päästäkseen johonkin haluaamansa ja määrittelemäänsä vaikutukseen. Näin ajattelemalla *hybridiuhka* -termi voidaan kääntää muotoon *hybridivaikuttaminen*. Uhka vai vaikuttaminen - puhumme samasta asiasta, vain eri näkökulmasta. Monien eri vaikuttamiskanavien ja -työkalujen käyttö omien etujen edistämiseksi - yleensä kohteen etujen kustannuksella - on kohteen kannalta uhka, mutta samalla tekijän kannalta vaikuttamista. Suojelupoliisi (2020) käyttää kansallisen turvallisuuden vuosikatsauksessaan juuri tätä hybridivaikuttamisen termiä, sisällyttäen siihen kuvion 1 mukaiset osakokonaisuudet.



KUVIO 1. Hybridivaikuttamisen käsite. (Suojelupoliisi, 2020)

On huomionarvoista, että Suojelupoliisi nostaa määrittelyssään esiin myös muiden toimien mahdollisuuden, jotka siis jätetään tarkemmin määrittelemättä. Tämän voi tulkita kuvastavan hybridiuhkan tai -vaikuttamisen käsitteen alati uudelleenmuovautuvaa luonnetta; ovi jätetään auki kaikelle sellaiselle toiminnalle, jota ei nykyhetkellä osata tunnistaa ja määritellä.

Suojelupoliisi tuo esiin myös näkökulman siitä, että näillä toimilla ei välttämättä pyritä juuri niiden toimeenpanohetkellä samaan aikaan vaikutusta, vaan niitä käyttämällä voidaan valmistella tulevaisuudessa tapahtuvaa vaikutamisoperaatiota. Eli kohteeseen vaikuttava toimija on rytmittänyt operaationsa ajallisesti välitavoitteisiin ja vasta lopuksi varsinaiseen tavoitteeseen.

Sotilastiedustelun puolella on myös määritelty ja konkretisoitu hybridiuhkakäsitettä. Puolustusvoimien sotilastiedustelun mukaan hybridiuhkakäsitteen sijaan voitaisiin puhua *laaja-alaisesta vaikuttamisesta* (Puolustusvoimat, 2021a, s. 12). Edelleen saman lähteen mukaan tällä käsitteellä tarkoitetaan ”kaikkia valtiollisen toimijan käytettävissä olevia suorituskykyjä ja välineitä, joilla se pyrkii vaikuttamaan kohteeseen edistääkseen ulko- ja turvallisuuspoliittisia päämääriään”. Hybridivaikuttaminen on siis tämän määrittelyn mukaan valtiollisen tason, tai siihen rinnastettavissa olevan tahon, toimintaa. Myös vuosina 2013–2019 Puolustusvoimien tiedustelupäällikkönä toiminut Harri Ohra-aho kertoo sotilastiedustelun kohteiden olevan pääsääntöisesti valtiollisia toimijoita, tai vähintään valtioon kytköksissä olevien organisaatioiden toiminta ja aikomukset (Ohra-aho, 2019, 21:00). Tietenkään sotilastiedustelun kohteita ja laaja-alaisen vaikuttamisen toteuttajia ei voi sanoa yhdeksi ja samaksi toimijajoukoksi, mutta tarkastelun kohteena olleissa sotilastiedustelun kuvauksissa korostuu tiedustelun kohteissa, ja siten Suomen (ulkoiseen tai sotilaalliseen) turvallisuuteen vaikuttavissa tahoissa, valtiollisen toimijuuden elementti.

Turvallisuusviranomaisiin kuuluva Rajavartiolaitos on myös viime vuosina ollut toimivaltuuspäivityksien kierteessä, jotta kyseisen viraston kyky vasta-

ta hybridiuhkiin paranisi (HS, 2017; Ruotuväki, 2017). Hallituksen esitys rajavartiolaitonlain, ulkomaalaislain sekä eräiden niihin liittyvien lakien muuttamisesta annettiin lausuntokierrokselle vuonna 2017 (HE 201/2017). Tässä lakiesityksessä heti ensimmäisessä tekstikappaleessa korostetaan lakimuutosten tarpeen taustalla olevan sen, että Rajavartiolaitos voi vastata Suomen turvallisuusympäristössä ilmeneviin uhkiin, ja että lakimuutos on tarkoitus saattaa pikimmiten voimaan (HE 201/2017, s. 1). Koska olemassa olevat toimivaltuudet eivät enää täysin kelpaa uhkiin vastaamiseen, voi siis päätellä, että turvallisuusympäristö on myös Rajavartiolaitoksen näkökulmasta muuttunut. On siis mielenkiintoista ottaa tiedustelutoimivaltaa käyttäviin viranomaisiin vertailukohtaa myös muista turvallisuusviranomaisista, kuinka he näkevät hybridi -termin. Rajavartiolaitoksen vuosikertomuksissa ei tätä termistöä käsitelty (ainakaan vuosien 2017–2020 välisissä julkaisuissa), kuten ei myöskään voimassa olevassa Rajavartiolaitoksen strategiassa. Määritelmä Rajavartiolaitoksen viitekehykseen löytyi vasta samaisesta lakiesityksestä (HE 201/2017), kuten myös Rajavartiolaitoksen vastuuministeriön (sisäministeriö) määrittelemänä (Sisäministeriö, 2019d). Mielenkiintoista on, että näissä määrittelyissä määritellään erikseen hybridivaikuttaminen ja -uhkat. Lakiesityksessä hybridivaikuttamiseksi katsotaan suunnitelmallinen toiminta, jossa valtiollinen tai ei-valtiollinen toimija hyödyntää monipuolisesti ei-sotilaallisia keinoja pyrkien vaikuttamaan valtion heikkouksiin ja saavuttamaan omat tavoitteensa (HE 2017/2017, s. 5). Edelleen lakiesityksessä hybridiuhkat taasen ovat sellaisia sisäisen tai ulkoisen turvallisuuden häiriötilanteita, joiden torjunta edellyttää usean viranomaisen yhteistyötä (HE 2017/2017, s. 5). Sisäministeriö (2019d) määrittelee hybridiuhkat tarkoittamaan erilaisia tahallisia tapoja aiheuttaa painetta, vahinkoa, epävarmuutta ja epävakautta kohteena olevalle valtiolle.

Tämän luvun tuloksena nähdään, että hybridivaikuttamisen kohteet ovat suomalaisen turvallisuusviranomaismäärittelyn mukaan pääsääntöisesti yhteiskunnallisen tason elementtejä. Ja edelleen vaikuttamisen toteuttajataho on joko suoraan valtiollinen toimija tai jokin valtion tukema taho. Näin ollen synteesinä voidaan lausua, että ainakin turvallisuusviranomaisten viitekehyksessä hybridivaikuttaminen on tavoitteellista valtiollisen tason toimintaa, jonka vaikuttavuus pyritään kohdistamaan toisen valtion yhteiskunnalliseen ja valtiolliseen tasoon, mutta vaikutustoimet itsessään voivat kohdistua monipuolisesti kohdevaltion jokaiselle tasolle aina yksilötasosta koko yhteiskuntaa koskettavaksi ilmiöksi. On huomattava, että valtio tässä määritelmässä voi tarkoittaa myös sen kaltaista toimijaa, eli ihmisyyhteisöä, jolla täyttyy ainakin osa näistä vaatimuksista: osoitettavissa oleva maa-alue, väestö, hallinto sekä kyky täyttää kansainväliset sitoumukset (nämä kriteerit vuonna 1933 solmitun Montevideon sopimuksen mukaisesti). Tällä täsmennyksellä katetaan muutamissa määrittelyissä esiintynyt termi ”ei-valtiollinen toimija”.

3 TUTKIMUSAINEISTO JA -MENETELMÄ, AINEISTON KOODAUS

Tässä pääluvussa käsitellään yksityiskohtaisesti valittu tutkimusaineisto sekä kerrotaan ankkuroidusta tutkimusmenetelmästä, joka on valittu tämän tutkielman tutkimusmenetelmäksi. Tämän jälkeen pääluvussa koodataan esitelty tutkimusaineisto valitulla tutkimusmenetelmällä. Koodauksen tulokset kerrotaan teoskohtaisesti tekstimuotoisesti (alaluvut 3.3.1 - 3.3.5) sekä visuaalisena käsitekarttana (liitteet 1 - 5), jotta tutkimusprosessi on mahdollisimman läpinäkyvä. Kyseisen koodausluvun päättää teoskohtaisten koodauksien jälkeen suoritettu kaikkien yksittäisten koodausten yhdistäminen varsinaiseksi hybridiuhkakäsitteeksi (alaluku 3.3.6 sekä liite 6).

Jo tässä vaiheessa on ilahduttavaa kertoa se, että vähintään osa tutkimusaineistosta on ajallisesti uudempaa tekstiä kuin itse tiedustelulait. Tämä tarkoittaa sitä, että tiedustelulakien valmisteluvaiheen aikana ei ole voitu tukeutua näihin tuorempiin aineistoihin, vaan käytössä on ollut sen aikainen tietämys ja käsitys kansallisista uhkista. Joten kun tässä tutkielmassa on käytössä myös tuoreempaa tutkimusaineistoa, niiden avulla voi hybridiuhkakäsitteen muodostamisen lisäksi arvioida myös sitä, kuinka tiedustelulait ovat kestäneet hybridiuhkien muuttuvaa luonnetta näiden muutamien vuosien aikana, mitä lakivalmisteluvaihe ja tutkimusaineistojen julkaisuvuodet kattavat.

3.1 Tutkimusaineisto

Tutkimusaihe valikoitui tutkijan ja työn ohjaajan välisten keskustelujen perusteella, aiheen herättäessä kiinnostusta tutkijassa. Käsiteltävät teemat olivat jo valmiiksi tutkijalle tuttuja, mutta vain yleisellä tasolla, joten tutkimustyö piti aloittaa perehtymällä aihealueen aineistoon yksityiskohtaisesti. Käytännössä se tarkoitti ensin esimerkiksi kartoitustyötä, minkälaisista aineistoista voi tutkimuskysymyksiin saada muodostettua luotettavan ja relevantin vastauksen.

Koska aineistolähtöisyys oli vahvana esillä jo heti tutkimusaiheen valinnan yhteydessä, oli selvää, että tutkielma on laadullinen tutkimus, jossa perehdytään syvällisesti valittuun kirjallisuusaineistoon.

Tutkielman aineiston voi tutkielman teemojen mukaisesti lokeroida kolmeen eri kategoriaan: hybridiuhkiin liittyvät lähteet, tiedustelulakeihin liittyvät lähteet, sekä kolmantena tiedusteluun ja turvallisuuskäsityksiin liittyvät teorialähteet. Kaksi ensimmäistä kategoriaa muodostavat tutkielman tutkimusaineiston. Näihin kahteen ensimmäiseen kategoriaan, eli tutkimusaineistoon, kuuluvia teoksia ja kirjoituksia on tietoisesti pyritty etsimään eri yhteisöistä ja eri kirjoittajilta, jotta vältytään siltä ongelmalta, että aineistomassa koostuisi keskenään ristiin viittaavista teoksista. Käytännössä tämä tarkoitti pyrkimystä siihen, että aineistoa on valittu niin kotimaasta, kuten valtionhallinnon tekstit, hallituksen lakiesitykset ja kotimainen tutkimus sekä tieteelliset artikkelit, mutta myös ulkomailta. Ulkomaisia dokumentteja valitessa pääsääntönä tässä tutkielmassa pidetään sitä, että aineisto on tieteellistä, kuten vertaisarvioitua sekä lähdeviitteet ovat merkittynä. Painettujen teosten osalta on pyritty valitsemaan sellaisia teoksia, jotka ovat jonkin tunnetun ja luotettavan kustannustalon kustantamia.

Tarkemmin nimettynä aineisto koostuu mainitussa kolmessa kategoriassa, kategorioittain eriteltynä, seuraavalla tavalla: ensimmäisenä kategoriana hybridiuhkien osalta aineisto koostuu Suomen valtionhallinnon virallisista kertomuksista ja julkaisuista. Suomen uhkakuvakenttää määritetään valtiollisella tasolla Yhteiskunnan turvallisuusstrategiassa (YTS, 2017) – vahvassa sidoksessa kansalliseen riskiarvioon (Sisäministeriö, 2019a) –, ulko- ja turvallisuuspoliittisessa selonteossa (Valtioneuvosto, 2020), puolustusselonteossa (Valtioneuvosto, 2017), sisäisen turvallisuuden selonteossa (Sisäministeriö, 2016) sekä ajantasaisessa hallitusohjelmassa (Valtioneuvosto, 2019). Näistä asiakirjoista hallitusohjelma on konkreettisten uhkakuvien näkökulmasta yleisimmällä tasolla oleva asiakirja, joka nivoo yhteen hallituksessa olevien puolueiden tavoitteet ja antaa näin pikemminkin yleiskuvan siitä, kuinka strategisella tasolla Suomen valtiota halutaan kehittää ja miten Suomi asemoi itsensä ympäristöönsä nähden – osana sitä myös uhkat ja turvallisuus. Tämän kategorian aineisto muodostaa sen tutkimusaineiston, jonka avulla muodostetaan tutkimuksen hybridiuhkakäsite.

Lisäksi tutkimusaineiston relevanttiuden varmistamiseksi, eli että kaikki valtiolliset uhkakuvia määrittävät tekstit ovat otettu huomioon, on tarkasteltu yhtä uhkakuva-aiheeseen liittyvää tietokirjaa. Tämä teos on Limnellin ja Ilo-niemen vuonna 2018 julkaistu *Uhkakuvat* -tietokirja. Valinta kohdistui tähän teokseen ensinnäkin siksi, että kyseisen teoksen tekijät ovat aihepiirin asiantuntumuksen osalta valtakuntamme kärkitutkijoita, teos tarkastelee suomalaista yhteiskuntaa, ja siinä on lähdeviitteet. Toisekseen teos on sen verran tuore julkaisu, että iso osa edelliskappaleessa mainituista selonteoista on ollut voimassa sen ilmestymisen aikaan. Tässä teoksessa kirjoittajat kertovat oman näkemyksensä siitä, mitkä asiakirjat määrittävät valtiollisen uhkakuvanarratiivin. Teoksessa käsitellään myös hybridiuhkia, eli teos voi toimia myös aiempina tutkimuksena. Tämän tutkielman häiriöttömän toteutumisen vuoksi *Uhkakuvat*

(2018) teosta ei kuitenkaan tarkasteltu hybridiuhkien osalta, vaan tutkielman hybridiuhkakäsite muodostettiin puhtaasti edellä mainittujen valtiollisten tekstien, primäärilähteiden, perusteella.

Toisena kategoriana olevat tiedustelulait ovat selkeärajainen tutkimusaineisto; tämä kategoria sisältää lakitekstejä keskeisine valmisteluteksteineen. Myös tämän kategorian lähteet kuuluvat tutkielman tutkimusaineistoon. Tiedustelulait käsittävät lain sotilastiedustelusta (590/2019) sekä lain tietoliikennetiedustelusta siviilitiedustelussa (582/2019), ja lisäksi eräitä muutoksia aiempiin, jo säädettyihin lakeihin (817/2018; 581/2019; 583/2019; 584/2019; 585/2019; 591/2019; 592/2019; 593/2019). Erityishuomiona mainittakoon lakimuutos 581/2019, joka sisältää muutoksia poliisilain (872/2011) eri lukuihin, sekä myös lisäyksen uudesta 5 a luvusta. Poliisilaki (872/2011) luvussa 5 a säädetään siviilitiedustelusta. Tiedustelulakeihin katsotaan kuuluvan myös laki tiedustelutoiminnan valvonnasta (121/2019). (Eduskunta, 2019; lakiviitteet lähdeluettelossa I-kirjaimen kohdalle listattuna)

Tässä tutkielmassa keskitytään kahteen uutena säädettyyn lakiin, eli lakiin sotilastiedustelusta sekä lakiin tietoliikennetiedustelusta siviilitiedustelussa. Lisäksi tutkielmassa otetaan lakimuutoksista huomioon laki poliisilain muutoksesta (581/2019), jonka keskeinen sisältö on poliisilakiin uuden luvun (5 a Siviilitiedustelu) lisääminen. Nämä kolme lakia yhdessä säättävät siviili- ja sotilastiedustelun kohteet, käytön edellytykset, sekä tiedustelumenetelmät, ja näistä syistä juuri nämä lait ovat otettu tutkielmassa tarkastelun kohteeksi.

Varsinaista lainsäädäntöä taustoittaa hallituksen esitykset eduskunnalle, jotka ovat tiedustelulakien osalta varsin laajoja, noin neljäsataasivuisia dokumentteja. Kaikki nämä edellä mainitut lait ja lakimuutokset ovat eduskunnassa hyväksytyt hallituksen esitysten pohjalta, eikä esimerkiksi kansanedustajan aloitteesta. Tässä tutkielmassa tarkastellaan myös näitä hallituksen esityksiä eduskunnalle niin siviili- (HE, 202/2017) kuin sotilastiedustelusta (HE, 203/2017). Tällä lakitekstien tausta-aineiston sisällyttämisellä lähdeaineistoon pyritään kasvattamaan tiedustelulakien tarkastelun ja koodaamisen luotettavuutta, sillä tutkielman tekijä voi tämän tausta-aineiston kautta syventää ymmärrystään tiedustelulaeista, jolloin riski lakitekstien väärintulkitsemiselle pienenee.

Kolmas kategoria on tutkielman lähdeaineistoa, ja tämän aineiston avulla muodostetaan tarvittava teoriapohja. Tähän aineistoon tutkielmassa nojautetaan esimerkiksi niissä kohdin, kun on tarve kuvata esimerkiksi tiedustelun teoriaa, tiedustelumenetelmiä tarkemmin kuin otsikkotasolla, hybridiuhkia tai jotain kyseisen uhkakäsitteen alakategoriaa. Näissä lähteissä on pyritty valitsemaan ulkomaisten luotettavien ja tunnettujen painotalojen julkaisemia teoksia, tai artikkeleita tieteellisesti vertaisarvioituista julkaisuista. Myös jo mainittu kotimainen uhkakuvateos (Limnell & Iloniemi, 2018) kuuluu tähän kategoriaan. Painotus ulkomaisiin lähteisiin on tietoinen valinta: mikäli teoriakuvauksissa-kin tukeuduttaisiin ainoastaan kotimaisiin lähteisiin, olisi riskinä ajautua tietynlaiseen aineistokuplaan. Tämä tarkoittaa, kun kotimaisen tutkimusaineiston perusteella muodostetaan hybridiuhkakäsite, ja edelleen sitä peilataan kotimai-

seen lainsäädäntöön, niin mikäli vielä käsiteltävien aiheiden teoriakin olisi kotimaista tekstiä, voisi syntyä tilanne, jossa päätutkimuskysymykseen vastataan suppean ja tietyn näkökulman (suomalaisuuden) omaavan aineiston pohjalta. Aineisto saattaisi olla lähteiden lukumäärällä laskettuna laaja, mutta todellisuudessa teosten, asiapapereiden ja julkaisujen takana saattaisi olla suppeakin asiantuntijajoukko; yhteiskuntamme on kuitenkin pieni, ja tiedustelun sekä hybridiuhkien kansallinen asiantuntijajoukko on rajallinen, jolloin lähdeaineiston muodostamisen takana saattaisi olla samoja tutkijoita ja asiantuntijoita. Ulkomaisilla lähteillä pyritään tuomaan luotettavuutta tutkielmaan sekä laadullista syvyyttä, kun synteisiä voidaan tehdä kotimaisten ja ulkomaisten lähteiden välillä.

Lisäksi tarkoituksensa tällä aineiston jaottelulla tutkimus- ja lähdeaineistoon on vielä se, että lähdeaineisto, johon viitataan pitkin tutkielmaa, on erotettu aiemmasta tutkimuksesta sekä itse tutkimusaineistosta. Tällöin tutkimusaineiston analyysin (eli koodauksen) jälkeen saatuja tuloksia voidaan peilata lähdeaineistosta esiin nousseihin seikkoihin ilman riskiä siitä, että eri aineistot olisivat tutkielman teon aikana sekoittuneet keskenään aiemmin. Ja tutkimuksen lopussa havaittuja tutkimustuloksia voidaan verrata aiemman tietellisen tutkimuksen tuloksiin, ja löytää mahdollisia samoja tuloksia (jolloin muodostettu tieto vahvistuu), tai toisaalta löytää ristiriitaisia tuloksia (jolloin muodostettuun tietoon lienee syytä suhtautua kriittisesti ja asettaa tulokset esimerkiksi jatkotutkimuksen alle). Seuraavaksi siirrytäänkin aiemman tutkimuksen esittelyyn.

3.2 Tutkimusmenetelmä

Tutkielma toteutetaan laadullisena tutkimuksena. Tutkielman aloitusasetelma on aineistolähtöinen, eli tutkielman alkulähteet ovat jo olemassa olevaa ja julkaistua kirjallista tietoa. Koska tutkielman keskiössä olevat molemmat ilmiöt, hybridiuhkat ja tiedustelulait, ovat tutkielman suomalaisessa viitekehyydessä uudehkoja ilmiöitä tai käsitteitä, on päätutkimuskysymykseen vastaamiseksi valittu käytettäväksi ankkuroitua tutkimusmenetelmää. Se on alkuperäisnimeään *grounded theory*, ja yleisenä lyhenteenä siitä käytetään kirjainparia GT. Tässä tutkielmassa käytetään tästä tutkimusmenetelmästä suomenkielistä termiä *ankkuroitu menetelmä*.

Ankkuroitu menetelmä sai syntynsä 1960-luvulla. Oppi-isinä toimivat Glaser ja Strauss vuonna 1967 julkaistulla teoksellaan (Glaser & Strauss, 1967), ja vaikka he myöhemmin kiistelivät metodin peruseriaatteistakin (ks. Glaser 1992), on metodissa ollut läpi sen olemassaoloajan useita yleisesti hyväksytyjä lainalaisuuksia. Yksi, ja metodin käyttötarkoitukseen liittyvä, ehto on se, että sitä tulee käyttää uusien teorioiden luomiseen aineistoa analysoimalla. Vastakohtana ankkuroidulle menetelmälle voi nähdä tutkimusmetodin, jossa hypoteesien testauksen kautta muodostetaan yleinen teoria, sillä ankkuroidussa

menetelmässä toinen yleisesti hyväksytty ehto on alkutilanteen hypoteesittomuus. (Silvonen & Keso, 1999, s. 88–89)

Tämän tutkimusmenetelmän yleisesti hyväksytyjen ehtojen lisäksi on tunnistettu myös tiettyjä ankkuroidun menetelmän malleja, tai malliversioita. Osaltaan nämä tutkimusmetodin eri kehityssuuntaukset johtuivat juuri siitä, että tutkijat kävivät keskinäistä debattia tavoista, joilla ankkuroitua menetelmää tulisi toteuttaa. Monessa ankkuroitua menetelmää analysoivassa tekstissä tunnistetaan kolme ankkuroidun menetelmän mallia (ks. esim. Sebastian, 2019), jotka ovat ensimmäisenä Barney Glaserin (1992) kehittämä klassinen ankkuroitu menetelmä (GT), toiseksi tulkitseva ankkuroitu menetelmä (*interpretive grounded theory*, IGT), jolle on myös muita nimityksiä kuten laadullinen aineistoanalyysi (*qualitative data analysis*) tai straussilainen ankkuroitu menetelmä (*Straussian grounded theory*). Tämä usean eri nimityksen menetelmä perustuu Straussin ja Corbinin yhteisteokseen (Corbin & Strauss, 2015). Ja kolmantena versiona on konstruktivistinen ankkuroitu menetelmä (*constructivist grounded theory*, CGT), jossa tekijänä on molempien Straussin ja Glaserin oppilas Kathy Charmaz (Charmaz, 2014). Hän julkaisi modernimmaksi kuvatun (Sebastian, 2019, s. 3) version ankkuroidusta menetelmästä, jossa on nimensä mukaisesti vaikutteita konstruktivistisesta tieteenfilosofiasta. Tässä versiossa tunnustetaan myös se, että tutkija ei voi sulkea pois aiempaa mahdollista tietoaan ja kokemustaan tutkimusaiheesta. Tämän vuoksi tässä tutkielmassa käytetty ankkuroitu tutkimusmenetelmä muistuttaa eniten tätä konstruktivistista ankkuroitua menetelmää, sillä tutkijalla on aiempaa perehtyneisyyttä hybridiuhkia käsitteleviin teksteihin, kuin myös valtiollisiin turvallisuuspoliittisiin julkaisuihin. Charmazin menetelmän mukaisesti valittu tutkimusaineisto koodataan kokonaan, ja koodauksen perusteella esiin nousevat teemat ryhmitellään merkittävimpiin kategorioihin (Sebastian, 2019, s. 4). Klassisen ankkuroidun menetelmän luonteeseen taasen kuuluu olla mahdollisimman irti kaikista tieteenfilosofisista suuntauksista ja tutkijan tulisi olla mahdollisimman erillään kaikesta tutkimusaiheesta aiemmin kirjoitetusta tiedosta (Sebastian, 2019, s. 4), joka ei aivan istu tähän tutkimukseen, koska seuraavassa alaluvussa esitellään juuri tämän tutkimuksen asemoitumista tieteenfilosofisessa kentässä.

Tutkimuksen alussa on siis tutkimusaineisto, jota ennakkoluulottomasti tulkitaan, *koodataan*, ja annetaan aineistosta nousevien seikkojen muodostaa teoria. Aineiston koodaus ja teoriaa muodostava analyysi kulkevat käsi kädessä, ja tutkimusmenetelmä on puhtaasti laadullinen; aineisto on tarkkaan valittu ja rajattu, ja sitä tulkitaan mahdollisimman syvällisesti, jopa sana sanalta. (Silvonen & Keso, 1999, s. 88–89)

Tämä menetelmä soveltuu käytännössä erityisen hyvin uusien aihepiirien tutkimukseen, joista on tutkimushetkellä saatavilla vasta vähän tutkittua, jäseneltyä tai koostettua tietoa. Tutkimusaineiston lisäksi muuhun tutkimusaihetta käsittelevään aineistoon ei tule paneutua tekstin koodausvaiheessa, koska silloin teorianmuodostus voi häiriintyä ja saada vaikutteita tutkimusaineiston ulkopuolelta. Tutkimuksen aikana voidaan siirtyä myös tähän muuhun aineistoon, mutta teorianmuodostuksen tulee olla siinä

vaiheessa, että tutkimuksen luotettavuus voidaan taata (Silvonen & Keso, 1999, s. 90). Tässä tutkielmassa perehdytään aiempaan, luvun 1.2 mukaiseen, aihealueen tutkimukseen vasta siinä vaiheessa, kun tutkimusaineisto on täysin koodattu. Käytännössä siis pääluke 4 on valmistunut ennen aiempaan tutkimukseen perehtymistä. Vasta viimeisessä pääluvussa, pohdintaosuudessa vertaillaan tämän tutkimuksen tuloksia aiempaan tutkimukseen, ja katsotaan, tukevatko tämän tutkimukset tulokset aiempaa tutkimusta, vai ovatko nämä tulokset kenties ristiriidassa. On toki syytä huomioida, että juuri tästä aiheesta ei ole aiempaa suomalaista tutkimusta.

Tässä opinnäytetyössä uhkakuvia käsitteleviä aineistoja koodamalla muodostetaan kansallinen uhkakäsite. Tämä käsite esitetään graafisen käsitekartan muodossa, jossa ydinkäsitteen *uhkakuvat* ympärille rakentuu avainkategorioita. Kategorioiden nimet täsmentyvät sitä mukaa, minkälaisia uhkia teksteistä nousee. Mikäli teksteissä esiintyy tietty kattokäsite yksittäisille uhkille, kuten vaikkapa kansalliset uhkat tai yksilöön vaikuttavat uhkat, niin nämä kattokäsitteet voidaan ottaa avainkategorioiksi. Kun on luotu kansallinen uhkakuvakäsite, se jalostetaan hybridiuhkakäsitteeksi (kuvio 3), eli kansallisesta uhkakuvakäsitteestä on otettu kaikki ne uhkat ja vaikuttamismekanismit, joissa taustalla on ihmisen tavoitteellinen toiminta. Tarkemmin tästä prosessista on kerrottu luvussa 3.3.6.

Näin tutkielman ensimmäinen pääteema on tullut täytetyksi, kun on muodostettu konkreettinen ja luotettava käsite hybridiuhkille. Ankkuroidun menetelmän mukaisella koodauksella analysoidaan ja käsitellään myös tiedustelulakeja esitöineen sekä lakiesityksineen, mutta niistä ei muodosteta samanlaista graafista käsitekarttaa, vaan sitä vertaillaan jo muodostettuun hybridiuhkakäsitteeseen. Tämä vertailu tapahtuu luvussa 4.1.

3.3 Hybridiuhkakäsitteen muodostaminen ankkuroidulla menetelmällä

Valitun tutkimusaineiston koodaamisprosessin aikana muodostettiin uhkatekijöiden avainkategorijaottelu. Samaa avainkategorisointia sovellettiin kaikkiin koodattuihin teoksiin. Tämä tehtiin siksi, jotta yksittäisten teosten koodaamisen lopputuotteet olisivat vertailukelpoisia keskenään, ja jotta niiden pohjalta voisi muodostaa lopullisen hybridiuhkakäsitteen. Kun yksittäiset teokset olivat tulleet koodatuksi – eli teosten käsitekartat olivat muodostettu – jokaisen koodaustuotteen yksittäiset uhkat vietiin lopulliseen hybridiuhkakäsitekarttaan. Yksittäisten uhkatekijöiden päällekkäisyydet poistettiin, eli vaikkapa kybervaikuttamista, joka tekijänä esiintyi jokaisessa koodatussa teoksessa, ei lopulliseen käsitekarttaan viety moneen kertaan. Lisäksi jos uhkatekijä toistui eri asiakirjoissa, mutta eri avainkategoriasissa, katsottiin mihin avainkategoriaan uhka useimmissa asiakirjoissa sijoittui, ja kyseinen

uhkatekijä kategorisoitiin lopulliseen hybridiuhkakäsitteeseen eniten suosiota saaneen avainkategorian alle.

Itse avainkategorioiden muodostaminen tapahtui tutkimusaineiston perusteella, ja lisäksi tukeuduttiin muutamiin sellaisiin teoksiin tai teoksien sisällä olevaan osaan, jossa käsitellään turvallisuuteen vaikuttavia tekijöitä. Nämä tukevat teokset ovat Sisäministeriön (2004) julkaisu sisäisestä turvallisuudesta sekä Linnélin ja Iloniemen (2018) teos siltä osin, mitä he käsittelevät sotiaallisten uhkakuvien murrosta kylmän sodan päätyttyä.

Avainkategorioista, niin ensinnäkin kansallisessa riskiarviossa listataan jo sisällysluettelossa monia tapahtumia, jotka ovat ihmisen toiminnasta riippumattomia (Sisäministeriö, 2019a). Näistä tapahtumista käytetään kyseisessä teoksessa nimitystä *häiriötilanne*. Vaikka tällaisten uhkien olemassaolo on usein tiedostettu, ei niiden tapahtumisen todennäköisyydelle usein voi ihminen mitään, ainoastaan seurauksien vakavuutta voi ihminen jossain määrin hallita. Esimerkki tämäntyyppisestä uhkasta on luonnonmullistukset, kuten maanjäristykset, niistä aiheutuvat tsunamit, tai vaikkapa tulivuorenpurkaukset. Linnélin ja Iloniemi (2018, s. 32) sijoittavat tähän kategoriaan myös ilmaston ääri- ja poikkeusilmiöt, vaikka niiden synnyn taustalla on välillisesti ihmisen toimet; kulutus- ja elintottumuksiemme myötä kasvaneet kasvihuonekaasupäästöt ja sen johdosta kiihtynyt ilmastonmuutos aiheuttamassa sään ääri-ilmiöitä. Ensimmäisenä uhkakategoriana on siis *ihmisistä riippumattomat uhkat*.

Perusteet muiden avainkategorioiden luontiin pohjautuu samantyyppiselle tapahtuma- ja ajatusketjulle, mikä tapahtui vuosituhaten vaihteen tienoilla yhteiskunnallisen turvallisuuskäsityksen laajentuessa. Tuolloisen yhteiskunnallisen turvallisuuskäsityksen murroksen keskeisiä muutostekijöitä olivat kylmän sodan päättymisen, YYA-sopimuksen raukeaminen ja Suomen EU-jäsenyys. Nämä tapahtumat avartivat Linnélin ja Iloniemen mukaan (2018, s. 61–62) turvallisuuskäsitys- ja uhkakeskustelua, ja länsimaisissa yhteiskunnissa tämä tarkoitti sitä, että kansallisia uhkakuvia alettiin sitomaan enenevässä määrin niin sanottuihin uusien uhkien käsitteeseen. Suomessa tämä näyttäytyi 2000-luvun alussa lyhyesti siten, että sotilaallisia uhkakuvia pidettiin vanhahtavina uhkakuvina, ja kaikkia muita uhkakuvia käsiteltiin uusina uhkakuvina (Linnélin & Iloniemi, 2018, s. 63). Tämä uhkakuvien muutoksen kehityskulku ei suinkaan ollut ajallisesti tarkkarajainen tapahtuma, vaan pikemminkin jatkuva prosessi, joka on edelleen käynnissä. Myös tämä tutkielma pyrkii hahmottamaan tätä uhkakuvien muuttuvaa luonnetta nyky maailmassa.

Mutta vaikka siis sotilaalliset uhkakuvat säilyivät Suomessa kansallisten uhkakuvien kirjossa, tunnistettiin meidän kaksinapaisen luonteen saanut uhkakuvajaottelu, toisaalta sotilaallisiin ja toisaalta kaikkiin muihin uhkiin aikansa eläneeksi. Eri uhkatekijöiden nähtiin olevan yhä vahvemmin keskinäisessä vuorovaikutuksessa. Erityisesti sotilaallisessa suunnittelussa käytetty uhkan voimakkuuden laskenta- ja määrittelykaava *tahto * kyky = uhka*, sinällään säilytti matemaattisen pätevyytensä, mutta samalla tunnistettiin, ettei

sen käyttökelpoisuus ole universaali. Uhkia tuli arvioida myös uhkan tuottajan motiivien näkökulmasta, kun siis olemme jo rajanneet ihmisestä riippumattomat uhkat pois, omaan kategoriaansa. Esimerkiksi terroristista toimintaa arvioitaessa, vaikka väkivaltaisen iskun kyvykkyys kohdistuisi yksittäisiin ihmisiin, uhkaaja haluaa vaikuttaa koko yhteiskuntaan pelkoa ja sekasortoa kylvämällä. (Limnell & Itoniemi, 2018, s. 19–21)

Kun uhkakuvajaottelu sotilaallisiin ja muihin uhkiin on nyt nähty vanhentuneeksi, on sen mukainen avainkategorisoiminen pois suljettu tässäkin tutkimuksessa. Toisena potentiaalisena vaihtoehtona tarkasteltiin jakoa sisäisiin ja ulkoisiin uhkiin. Mutta kun jo sisäisen turvallisuuden tutkimuksissa (ks. esim. Rumbin, 2020, s. 19) nähdään perusteltuna asettaa koko sisäisen turvallisuuden käsite kritiikin alle, ja todetaan että kyseinen käsite on luotu palvelemaan poliittista toimintaa sekä päätöksentekoa (esim. budjettirahoituksen määrittämisen osalta), ei tämäkään jakoperuste ole kestäväällä pohjalla tämän tutkielman viitekehyksessä.

Sisäministeriö (2004, s. 14) määrittelee sisäisen turvallisuuden tarkoittamaan sellaista yhteiskunnallista tilaa, jossa yhteisön jäsen voi ilman pelkoa ja turvattomuutta nauttia oikeusjärjestelmän hänelle tarjoamista vapauksista ja oikeuksista. Kun olemme jo tunnistanee, että tätä yhteiskunnallista turvallisuutta voivat horjuttaa niin yhteiskunnan sisältä nousevat uhkat, kuin myös yhteiskunnan ulkopuolelta tulevat uhkat, oli lopulta syytä tarkastella potentiaalista avainkategorijakoa *yhteiskuntatason uhkiin* sekä *globaaleihin uhkiin*. Globaalit uhkat tässä yhteydessä tarkoittaa yhteiskunnan ulkopuolelta tuleviin, yhteiskunnassamme vaikutusta aiheuttaviin uhkiin. Tätä jakoa yhteiskuntatason sekä globaaleihin tukee myös luvussa 2.4 turvallisuuskäsitettä tarkasteltaessa esitetty näkemys siitä, että globaalit uhkakuvat ovat yhä kiinteämmin osa yksittäisen valtion uhkakuvia. Lopullisen sinetin tämä jako sai tutkimusaineiston koodauksen perusteella, kun yhteiskunnan turvallisuus sanana nousee lukumääräisesti monin kertaisesti esiin verrattuna sisäiseen turvallisuuteen (esim. Yhteiskunnan turvallisuusstrategiassa 'yhteiskunta' noin 200 hakuosumaa versus 'sisäinen' noin 15 osumaa).

Näin tässä tutkielmassa päädyttiin muodostamaan avainkategorijako *ihmisistä riippumattomiin uhkiin*, *yhteiskuntatason uhkiin* sekä *globaaleihin uhkiin*, ja kuviossa 2 visualisoidaan näiden kahden jälkimmäisen kategorian asemaa uhkatekijöiden kokonaisuudessa. Kuviossa avainkategorista toiseen ja samalla ylöspäin etenevällä nuolella halutaan kuvata kategorioiden keskinäistä hierarkiaa. Alhaalla on yksityiskohtaisempi taso, josta edetään kohti ylätasoa, jossa sijaitsee yleismaailmallisempi, eli globaali uhkakategoria.



KUVIO 2. Uhkakategoriat yksilöstä globaaliin.

Seuraavissa alaluvuissa esitetään kunkin tutkimusaineistoteoksen koodaus sijoittaen niistä löytyvät uhkatekijät näihin avainkategorioihin, ja viimeisessä alaluvussa 3.3.6 muodostetaan yksittäin ja toisistaan erillään koodatuista teoksista yhdistetty kansallinen uhkakuvakäsitekartta (tämä käsitekartta on liitteessä 6). Tässä käsitekartassa on mainittu kaikki teoksissa olevat uhkat. Kuitenkin selkeyden kannalta kaikkia löydettyjä uhkia ei suinkaan ole pelkästään listamaisesti lueteltu ja ynnätty yhteen käsitekartaan, vaan yhdistämistä ja synteisiä on tehty. Tarkempi kuvaus prosessista on kyseisessä alaluvussa.

Ja on syytä korostaa, että tämä erillisten teosten perusteella johdettu kansallinen uhkakuvakäsitemalli on eri asia kuin kansallinen hybridiuhkakäsitemalli. Koska tutkielman fokusessa ei kuitenkaan ole kansallisen uhkakuvakäsitemallin muodostaminen, pyritään kyseinen termi pitämään pienessä asemassa siten, ettei sitä nosteta pää- tai alalukujen otsikoihin. Eli kansallinen uhkakuvakäsitemalli on vain välitavoite, ja vasta siitä johdettu hybridiuhkien käsitemalli on varsinainen tavoite – eli vastaus tutkielman yhteen tutkimuskysymykseen. Myös tämä hybridiuhkakäsitemalli muodostetaan tämän luvun 3.3 viimeisessä alaluvussa 3.3.6.

3.3.1 Hallitusohjelma

Tässä tutkielmassa tarkastellaan ja koodataan tekoheikellä voimassaolevaa hallitusohjelmaa (tulokset liitteessä 1), joka on pääministeri Sanna Marinin hallitusohjelma 10.12.2019. Huomionarvioista on, että kyseessä on alunperin kesäkuussa 2019 julkaistu hallitusohjelma, pääministeri Antti Rinteen

hallituksen ohjelma. Pääministeri Sanna Marin otti kyseisen hallitusohjelman omakseen kun tasavallan presidentti myönsi eron Antti Rinteen hallitukselle joulukuussa 2019, ja nimitti samalla Sanna Marinin hallituksen. (Valtioneuvosto, 2019, s. 5)

Hallitusohjelmalla katsotaan olevan kaksi keskeistä tehtävää: sen avulla tuodaan esiin tieto hallituspuolueiden poliittisista aikomuksista, ja ohjelman myötä lujitetaan hallituskoalition keskinäistä kumppanuutta sitouttamalla kaikki puolueet samojen tavoitteiden saavuttamiseen (Mykkänen & Virtanen, 2020, s. 202). Näin koko hallitusohjelma asiakirjana ei ollut relevantti koodaustyössä, vaan uhkakuvia käsiteltiin asiakirjan johdantoluvussa, sekä luvuissa 2 (Kestävän talouden Suomi) ja 3 (Strategiset kokonaisuudet). Toki kuitenkin koko asiakirja tarkasteltiin läpikotaisin, ja tämä huomio uhkakuvien painottumisesta asiakirjan alkupuoliskolle tulikin ilmi koko asiakirjan kattavan koodauksen johtopäätöksenä.

Tämän, hallitusvastuuta kantavien eri poliittisten toimijoiden yhteensitomisen lisäksi Suomessa on viime vuosikymmeninä viety hallitusohjelmaa suuntaan, jossa se on entistä enemmän hallituksen toimintaa sitova ja ohjaava toimintasuunnitelma symbolisen yhteisen tahdonilmauksen sijaan. Ylipäätään hallituksen rooli halutaan nähdä, ja sitä se nykyään pitkälti onkin, strategisena toimijana, joka ohjaa kansallista politiikan tekoa. Hallituksen tulee ohjata politiikan tekoa poikkihallinnollisella perspektiivillä, hakien linjauksillaan vaikuttavuutta yli vaalikausirajojen. (Mykkänen & Virtanen, 2020, s. 202–210)

Näin ollen hallitusohjelma on asiakirja, josta kansallisen uhkakuvakäsityksen koodaus ja muodostaminen alkaa. Hallitusohjelma-asiakirjan rooli on tarkastelun kohteena olevien valtiollisten asiakirjojen hierarkiassa ylin, ja tähän tutkielmaan valitussa koodausjärjestyksessä on pyritty mukailemaan tätä hierarkiajärjestystä poikkihallinnollisista ohjaavista asiakirjoista kohti ministeriökohtaisia selontekoja. Myös Limnell & Iloniemi (2018, s. 72) tunnistavat hallitusohjelman tarkastelun tärkeyden, kun halutaan määrittää, minkä asioiden nähdään uhkaavan tai horjuttavan kansallista turvallisuutta.

3.3.2 Yhteiskunnan turvallisuusstrategia ja kansallinen riskiarvio

Yhteiskunnan turvallisuusstrategia on yksi valtioneuvoston periaatepäätöksistä. Asiakirjana periaatepäätöksen luonnehditaan olevan varsinaisia päätöksiä valmisteleva, ja suuntaviivoja antava, dokumentti. Tällä asiakirjatyypillä valtioneuvosto siis antaa ohjausta muulle valtionhallinnolle siitä, mihin suuntaan Suomea tulisi poliittisilla päätöksillä viedä, ja mikä on meidän tavoitetilä. (Valtioneuvosto, 2021)

Yhteiskunnan turvallisuusstrategia antaa ohjausta ja suuntaviivoja valtiomme varautumistyön järjestämiseen. Strategiassa kuvataan kokonaisturvallisuuden malli, eli strategia on luonteeltaan poikkihallinnollinen, ja soveltuu siten varautumistyön työkaluksi hallinnonalasta riippumatta.

Kokonaisturvallisuus -termin käyttö korostaa myös muiden sektoreiden – kuten elinkeinoelämän, järjestöjen ja kansalaisten – sisällyttämistä tähän varautumistyöhön, kuin pelkästään valtionhallinnon. (YTS, 2017, s. 5–6).

Tämä varautumistyö, jota Yhteiskunnan turvallisuusstrategia ohjaa, tarkoittaa niitä kaikkia toimia ja suunnitelmia, joita tehdään yhteiskuntamme häiriötiloja tai poikkeusoloja varten – ja niiden aikana. Tavoitteena näillä toimilla on ylläpitää yhteiskuntamme elintärkeitä toimintoja oikeusvaltioperiaatteesta kiinni pitäen (YTS, 2017, s. 9). Jotta kuvatus kaltaista varautumistyötä voidaan ylimmällä, strategisella tasolla ohjata, täytyy määrittää, mihin uhkiin varaudutaan. Sitä varten laaditaan kolmen vuoden väliajoin kansallinen riskiarvio, ja voimassa oleva Yhteiskunnan turvallisuusstrategia (YTS, 2017) käyttää vuoden 2015 kansallista riskiarviota. Tämän tutkielman laatimishetkellä on julkaistu uudempi riskiarvio, vuonna 2018.

Tässä tutkielmassa koodataan Yhteiskunnan turvallisuusstrategian sijaan itse uhkakuvien alkulähde, johon turvallisuusstrategia nojautuu edellä kuvatulla tavalla, eli kansallinen riskiarvio 2018 (Sisäministeriö, 2019a). Koodauksen tulokset ovat esitetty liitteessä 2. Kansallisen riskiarvion mukaisessa uhkakuvakäsitteessä huomataan ainutlaatuisuutta verrattuna kaikkien muiden asiakirjojen koodauksien lopputuotteisiin. Tässä asiakirjassa korostetaan erityisellä yksityiskohtaisuudella yhteiskunnan elintärkeiden ja kriittisten toimialojen ja sektoreiden häiriöriskiä, toimialoittain erikseen mainittuna.

Tarkasteluperspektiivi uhkakuvia kohtaan on asiakirjassa kuitenkin säilynyt monipuolisena ja kattavana, sillä vaikka yhteiskunnallisen tason uhkia eritellään varsin yksityiskohtaisesti, myös globaaleja ilmiötason uhkia sekä ihmisestä riippumattomia uhkia on tuotu esiin.

3.3.3 Ulko- ja turvallisuuspoliittinen selonteko

Poikkihallinnollisten strategioiden ja ohjelmien jälkeen tutkielmassa koodataan hallinnonalakohtaisia selontekoja. Nämä selonteot painottuvat kuvaamaan kyseisen hallinnonalan erityispiirteitä, ja ne toimivat pohjana muun muassa varsinaisille kyseisen hallinnonalan toimeenpano- ja seurantaohjelmille.

Ensimmäisenä selontekona on koodattu ulko- ja turvallisuuspoliittinen selonteko (Valtioneuvosto, 2020), jonka tulokset ovat esitetty liitteessä 3. Suomen ulko- ja turvallisuuspolitiikan painopisteisiin kuuluu turvallisuuden vahvistaminen niin kotimaassa kuin lähialueillamme, sekä myös muualla Euroopassa ja maailmassa (Valtioneuvosto, 2020, s. 24). Todennäköisesti tästä johtuen selontekoa koodatessa valtaosa uhkista ja turvallisuutta horjuttavista tekijöistä asettui koodauksen lopputuotteessa avainkategoriaan ‘globaalit uhkat’. Nämä tähän kategoriaan listatut tekijät olivat selonteossa esitelty niin yksiselitteisesti ns. globaalien näkökulman alla, ettei muuta vaihtoehtoa jäänyt. Valtaosa selonteon kertomista uhkista on lueteltu luvussa ”3.1 Globaalit haasteet ja muutosilmiöt”.

Selonteossa lausutaan, että Suomen ulko- ja turvallisuuspolitiikassa nähdään, että turvallisuuden globaali ja kansallinen ulottuvuus linkittyvät toisiinsa. Emme voi turvallisuuttamme vahvistaa pelkästään kansallisin toimin, vaan tämä työ edellyttää kansainvälistä turvallisuusyhteistyötä. Lisäksi selonteon mukaan monille turvallisuutta haastaville ilmiöille on yhteistä se, että ne ovat toisiinsa linkittyneitä ilmiöitä, vaikka niiden syntyapaikat eivät olisi täsmällisesti osoitettavissa samaan yhteen sijaintiin. (Valtioneuvosto, 2020, s. 24)

Nämä linjanvedot ovat hyvä ymmärtää tulkittaessa tämän asiakirjan koodausta, sillä ne selittävät vallitsevaa turvallisuuspoliittista ajattelutapaa. Globaali näkökulma on isossa painoarvossa, koska globaaleihin turvallisuushaasteisiin vastaamalla parannamme myös kansallista turvallisuuttamme.

3.3.4 Sisäisen turvallisuuden selonteko

Koodauksen lopputuote valtioneuvoston selonteosta sisäisestä turvallisuudesta on esitetty liitteessä 4. Tämän selonteon vastuutaho on Sisäministeriö, ja kyseessä on ensimmäistä kertaa laadittu selonteko valtiomme sisäisestä turvallisuudesta (Sisäministeriö, 2016, s. 6). Selonteko on jaettu kolmeen osaan, josta ensimmäisessä kuvataan turvallisuusympäristö, jossa Suomi toimii. Toisessa osassa kerrotaan kyseisen hallinnonalan turvallisuussuorituskykyjen sen hetkisestä tilasta ja kehittämissuunnitelmista, ja kolmannessa osassa analysoidaan selonteon aikana voimassa ollutta hallitusohjelmaa Suomen sisäisen turvallisuuden kannalta.

Kuten jo edellisten asiakirjojen koodauksen aikana tuli esille, turvallisuuden käsitteeseen liitetään Suomessa vahvasti ajatus uhkakentän monimutkaistumisesta. Tässäkin asiakirjassa useat esitetyt uhkat ovat sellaisia, että niiden syntyyn vaikuttaa paljon tekijät, jotka ovat Suomen valtion ulkopuolella. Näin ollen jaottelu sisäisiin ja ulkoisiin uhkiin on problemaattinen. Problemaattisuus konkretisoituu hyvin selonteon ensimmäisessä osassa, jossa Suomen turvallisuusympäristön kuvaus aloitetaan kansainvälisellä tarkastelutasolla; siis vaikka asiakirjan tarkoitus on ohjata yhteiskuntamme sisäisen turvallisuuden työtä, on toimintaympäristökuvaus aloitettava globaalista perspektiivistä (Sisäministeriö, 2016, s. 11–13). Tämä globaalista tarkastelutasosta aloittaminen johtuu siitä, että selonteon mukaan useiden yhteiskunnallisten uhkiemme sekä astetta matalampien turvallisuushuolien taustalla vaikuttaa loppujen lopuksi kuitenkin valtiomme rajojen ulkopuolella sijaitsevat tekijät (Sisäministeriö, 2016, s. 14).

Selonteon uhkakuvauksissa painotetaan siis yhteiskunnallisen tasoon. Läpi uhkakuvausten korostetaan Suomen turvallisuusympäristön ja uhkakuvakentän monimutkaistumista. Se johtaa selonteon mukaan muun muassa siihen, että tulevaisuuden ennustaminen vaikeutuu, ja muutosta parempaan tai turvallisempaan suuntaan ei voida nähdä. Yhteiskuntamme sisäisen turvallisuuden kuvauksessa korostuu ihmisten tuntemuksien merkitys. Turvattomuuden tunne on kasvanut ja yleistynyt monien eri tekijöiden

summana. Näitä tekijöitä ovat muun muassa haastava kansainvälinen turvallisuustilanne, näkyvät mutta yksittäiset järjestyshäiriöt sekä turvapaikanhakijoiden määrän kasvu. Tämänkaltaisessa kehityskulussa nähdään selonteossa isona riskinä se, että turvattomuuden tunteen lisääntymisen edelleen voimistuessa ja levitessä kansalaisten keskuudessa, se lisäänee yhteiskuntamme yleistä negatiivista ilmapiiriä ja voimistaa kansalaisten keskinäistä vastakkainasettelua (Sisäministeriö, 2016, s. 14).

3.3.5 Puolustusselonteko

Viimeisenä valtiollisena asiakirjana koodataan valtioneuvoston puolustusselonteko (tulokset liitteessä 5). Selonteon tarkoituksena on muodostaa valtiomme puolustuspoliittiset linjaukset ja antaa perusta Suomen puolustuskyvyn ylläpidolle, kehittämiselle ja käytölle (Valtioneuvosto, 2017, s. 4). Tämä on ainoa koodattu asiakirja, joka pidäytyy tiiviisti vain oman hallinnonalan toimintaympäristön uhkakuvien kertomisessa; esimerkiksi ihmisestä riippumattomia uhkia ei selonteossa kerrota ollenkaan. Tämä korostaa tärkeyttä usean valtiollisen asiakirjan tarkasteluun, kun halutaan muodostaa mahdollisimman kattava uhkakuvakäsite.

Toisaalta taas sotilaallisia, tai laiveammin ilmaistuna, voimapoliittisia uhkakuvia tässä asiakirjassa käsitellään kattavammin kuin missään muussa koodatussa teoksessa (voimapolitiikasta, ks. esim. Blombergs 2013). Myös tässä asiakirjassa tunnistetaan uhkakuvien ja turvallisuusympäristön monimutkaistuminen, mutta hieman eri perspektiivistä aiempiin koodattuihin teoksiin verrattuna. Selonteon tavoitteisiin nähden (puolustuspolitiikan linjanvedot) tekstissä käsitellään monimutkaistumista johdonmukaisesti sotilaallisesta näkökulmasta sanavalinnoin *sodan kuvan monipuolistuminen* sekä *sotilaallisen epävarmuuden lisääntyminen* (Valtioneuvosto, 2017, s. 5, 8).

Selonteon alkuosassa, pääluvut 1 ja 2, keskitytään turvallisuusympäristön sekä uhkakuvien kerrontaan. Loppuosa, pääluvut kolmesta viiteen, keskittyy poliittisen ohjauksen antamiseen puolustuskyvyn käytön, ylläpidon sekä kehittämisen suhteen.

3.3.6 Kansallisesta uhkakuvakäsitteestä johdettu hybridiuhkakäsite

Hybridiuhkakäsitteeseen liittyy ainakin suomalaisessa määrittelyssä pääsääntöisesti vaikuttamisen elementti, mihin johtopäätökseen päädyttiin tarkastellessa nykyisiä hybridiuhkamääritelmiä (luku 2.5). Tässä tutkielmassa ei tutkimusvaiheessa tehdä poikkeusta tästä yleisestä tulkinnasta, vaan tunnistetaan, että myös tutkimusaineistossa hybridiuhkiin liitetään tavoitteellisen toiminnan elementti.

Periaatteessa hybridiuhkat voisivat olla yksi avainkategoria kokonaisvaltaisen uhkakuvakäsitteen alla. Nyt siis tässä tutkimuksessa uhkakuvakäsitteen avainkategorioihin nousivat yhteiskunnalliset uhkat, globaalit uhkat ja ihmisestä riippumattomat uhkat. Mutta kun

hybridivaikuttamisen luonteeseen kuuluu käyttää kaikkia mahdollisia väyliä ja tapoja vaikuttaa kohteeseen, olisi visuaalisesti haastavaa esittää se yhtenä avainkategoriana samassa grafiikassa muiden kolmen avainkategorian kanssa. Sillä kun omien tavoitteiden saavuttaminen toteutetaan hybridivaikuttamisen keinoin, hyväksikäytetään globaaleja trendejä ja ilmiöitä, etsitään kohteen yhteiskunnan heikkoja kohtia ja voidaan vielä hyödyntää tapahtuneita onnettomuuksia ja muita ihmisestä riippumattomia tapahtumia, hybridivaikuttaminen läpileikkaa kaikki muodostetut avainuhkakategoriat. Eli hybridiuhkiin kuuluu uhkatekijöitä ja vaikuttamismekanismia kaikista kolmesta avainkategorista.

Vaikka hybridiuhkakategoria tästä huolimatta sijoitettaisiin uutena kategoriana edellisten jatkoksi, ongelmallisuus ei pysähtyisi pelkkään visuaaliseen haasteellisuuteen. Kolme muuta avainkategoriaa eivät voisi olla enää nyt nimetyin kaltaisia, koska aina kun hybridiuhkia löytyy näistä kolmesta kategoriasta, ne siirretään pois alkuperäisistä kategorioista hybridiuhkien kategoriaan, jolloin alkuperäiset kategoriat muodostuisivat puutteellisen kuvauksen antaviksi. Esimerkiksi yhteiskuntatason uhkat -kategoriaan, jos tässä lopputulemassa jäisi vaikkapa 1/4 -osa siellä alunperin olleista uhkista, ei se enää tosiasiallisesti kuvaisi yhteiskuntatason uhkia.

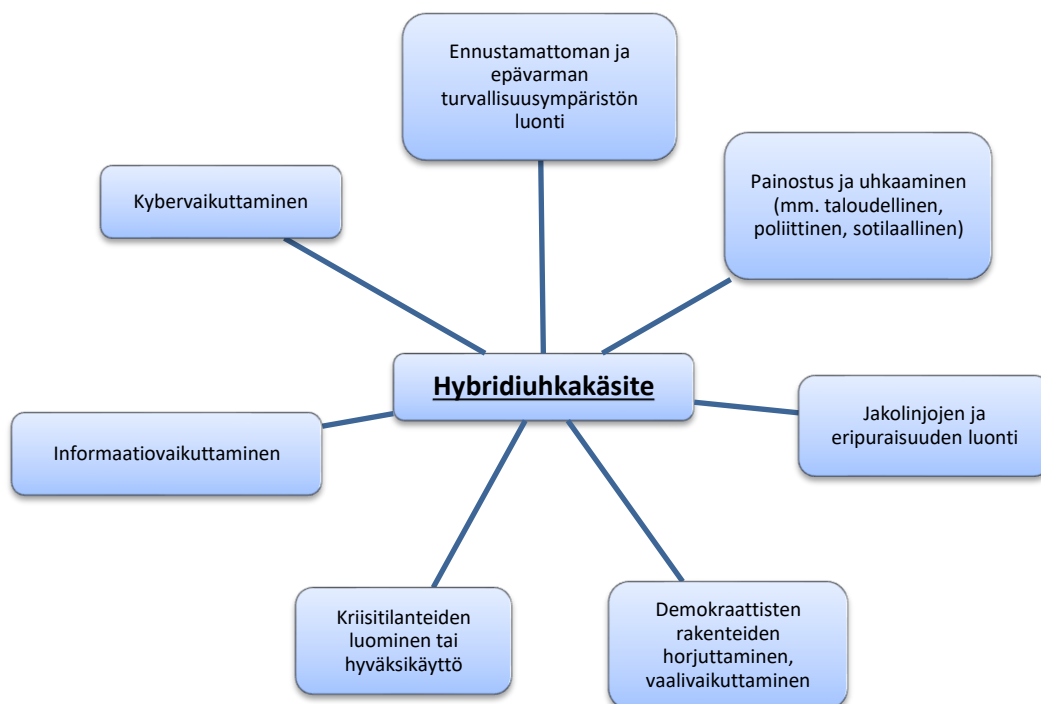
Näin ollen on syytä muodostaa sellainen hybridiuhkakäsite, johon koostetaan kaikki ne vaikuttamisen väylät ja keinot, eli yksittäiset uhkatekijät, jotka tutkimusaineiston mukaisissa asiakirjoissa luetellaan turvallisuuttamme heikentäviksi tai muuten yhteiskuntaa horjuttavaksi. Avainkategorioita ei hybridiuhkakäsitteen alle muodosteta, vaan kuten kerrottua, pelkästään yksittäisiä uhkatekijöitä. Liitteen 6 mukaisessa kansallisessa uhkakuvakäsitteessä hybridiuhkatekijä jo itsessään on avainkategorian omainen uhkatekijä, sillä sen yhteyteen on kirjoitettu yksittäisiä eri vaikutusmekanismeja, joita ei kuitenkaan voinut nostaa omiksi uhkatekijöikseen, sillä ne ilmaistiin tutkimusaineistossa pelkästään osana hybridivaikuttamista tai -uhkaa. Myös näiden tarkentavien vaikutusmekanismien poisjättäminen olisi ollut ongelmallista, sillä tutkimusaineistossa hybridivaikuttamisen välittömässä yhteydessä mainittiin nämä yksittäiset uhkatekijät.

Seuraavaksi, tämän alaluvun päätteeksi, esitellään tutkielmassa muodostettu hybridiuhkakäsite (kuvio 3). Tätä käsitekarttaa ei ole lisätty tutkielman loppuun omaksi liitteeksi, vaan se tuodaan osaksi tutkielman leipätekstiä, jotta tämän käsitekartan asema korostuu. Muut, liitteissä olevat käsitekartat ovat yksittäisten tutkimusaineistojen koodauksia, mutta tämä käsitekartta on kaikkien näiden yksittäisten koodausten yhdistetty lopputuote.

On syytä kuitenkin avata vielä prosessi, jolla hybridiuhkakäsite muodostettiin. Tämä tuo läpinäkyvyyttä tutkimukseen, sekä mahdollistaa tutkimuksesta ulkopuolisen henkilön muodostaa selkeän ja käsityksen siitä, kuinka vaihe vaiheelta hybridiuhkakäsite luotiin. Ensinnäkin, kokonaisuuhkakäsitteestä ei vain poimittu kaikkia niitä uhkia, joiden syntyyn tarvitaan ihmisen toimintaa (kuten sotilaallinen uhka), tai joita ihminen voi

omalla toiminnallaan eskaloida (kuten ilmastonmuutos). Tällainen kopioi-liitä mentaliteetti olisi johtanut todennäköisesti visuaalisesti isoon ja sisällöllisesti toistoa sisältävään hybridiuhkakäsitteeseen. Eli samankaltaisia uhkakuvauksia yhdistettiin yhdeksi hybridiuhkien alakäsitteeksi, pitäen samalla huolta siitä, että eri sanamuotojen yhdistyessä yhdeksi, tulee kuitenkin kaikkien alunperin käytettyjen sanamuotojen henki ja merkitys esiin. Esimerkkinä tästä yhdistelystä voi mainita uhkan häiriöistä yhteiskunnan kriittistä infrastruktuuria kohtaan, mikä uhka on liitteessä 2 (kansallinen uhkakuvakäsite kansallisen riskiarvion mukaisesti) eritelty toimialasektoreittain. Ja liitteessä 4 (kansallinen uhkakuvakäsite sisäisen turvallisuuden selonteon mukaisesti) tämä uhka on mainittu vain yhtenä uhkakäsitteenä 'kriittiseen infrastruktuuriin kohdistuvat onnettomuudet'. Näiden kahden eri selonteon samaa tarkoittavan uhkan voisi yhdistää muotoon 'kriittisen infrastruktuurin häiriötilat', koska ensinnäkin saman kattokäsitteen *kriittinen infrastruktuuri* alle lukeutuu kaikki erikseen mainitut toimialat. Ja toisekseen onnettomuus, kuten laaja tulipalo, aiheuttaa häiriön kyseisessä infrastruktuurissa. Mutta häiriö voi tulla myös muualta kuin onnettomuudesta, kuten käyttäjävirheestä. Eli häiriö on laajempi käsite kuin onnettomuus, kuitenkin sisältäen onnettomuuden, joten häiriö - termi on syytä säilyttää onnettomuuden sijaan.

Näin toimimalla saatiin hybridiuhkakäsite luotua kuvaamalla sitä seitsemällä alakäsitteellä (kuvio 3). Ja edelleen on syytä alleviivata, että pääkriteerinä hybridiuhkakäsitteeseen pääsemiseksi on se, että kyseisen yksittäisen uhkan toteutumiseen tarvitaan ihmisen tavoitteellinen toiminta, eli vaikuttaminen. Edellä mainittu esimerkki häiriötiloista kriittisessä infrastruktuurissa ei ole sellaisenaan mukana hybridiuhkakäsitteessä, vaan tämä yksittäinen uhkavektori on muokattu yleisempään muotoon. Tässä alaluvussa esitellyssä käsitteessä ei siis ole tarkoituksena se, että siinä kuvattaisiin tiettyjä yksilöityjä toimijoita, vaan kuvauksissa pyritään esittämään vaikutuskeinoja. Nyt käytetyn kriittisen infrastruktuuriesimerkin mukaisen uhkavektorin voi sisällyttää hybridiuhkan alakategoriaan 'kriisitilanteiden luominen tai hyväksikäyttö'. Mikäli kriittiseen infrastruktuuriin olisi vaikutettu tietoverkkohyökkäyksen keinoin, menisi se tapahtuma myös 'kybervaikuttaminen' alakategoriaan. Eli tässä käsitteessä on pyritty pois yksityiskohtaisuudesta, kohti yleistämistä, jolloin käsitettä voi soveltaa kukin yksittäinen toimija omista lähtökohdistaan kysymällä kysymyksen "kuinka nämä vaikutusmekanismit voivat toteutua minun organisaatiossa tai hallinnoimissani palveluissa/infrastruktuurissa?".



KUVIO 3. Hybridiuhkien käsittekartta

Tässä kappaleessa kerrotaan vielä lyhyesti kustakin seitsemästä uhkakategoriasta. Ensimmäisenä kategoriana tarkasteellaan *ennustamattoman ja epävarman turvallisuusympäristön luonti* -kategoriaa. Tähän kategoriaan koostui yksittäisiä uhkatekijöitä lähes jokaisen tutkielman liitteissä olevista uhkakuvakäsitteistä. Ennustamattomuus ei sanana suoraan esiinny tutkimusaineistossa uhkakuviin liittyen, vaan tämä sanamuoto on lopputulos uhkatekijästä 'turvallisuusympäristön monimutkaistuminen ja monipuolistuminen'. Sillä kun jompikumpi tai molemmat näistä sanoista esiintyvät yhdessä tai useamassa kohtaa jokaista tutkimusaineistodokumenttia, tuli tälle uhkatekijälle antaa painoarvoa myös tämän käsitteen luomisen yhteydessä tutkimalla tarkemmin, mitä tämä monimutkaistuminen tarkoittaa. Jo koodattua tutkimusaineistoa tarkastellessa kävi ilmi, että monimutkaistumisen termillä tarkoitetaan turvallisuustekijöiden ja -ympäristön odottamatonta kehityskulkua, jolloin aiemmin arvioitu ja oletettu tulevaisuuskehitys on sittemmin osoittautunut virheelliseksi arvioksi (ks. esim. Sisäministeriö 2016, s. 17). Monimutkaistumisella tarkoitetaan myös kasvaneita vaatimuksia turvallisuusympäristön analysointikykyyn (Valtioneuvosto, 2020, s. 11). Näin hybridiuhkien ja -vaikuttamisen kentässä voidaan ruokkia tätä nykymaailmassa turvallisuutta horjuttavaa ilmiötä joko luomalla uusia, odottamattomia turvallisuusjännitteitä tai eskaloimalla olemassa olevia kiistanaiheita uusille tasoille. Viimeaikaisia tapausesimerkkejä, jotka voidaan sijoittaa tähän kategoriaan, on muun muassa 2010-luvulla Itämeren ilmatilassa tapahtuneet turvallisuutta heikentäneet niin sanotut pimeät lennot sotilaskoneilla (LVM, 2015). Myös määrääjoin toistuvat isot sotaharjoitukset Itä-

Euroopan alueilla kuten Valko-Venäjällä, Venäjän länsiosissa sekä Suwalkin käytävän alueella herättävät aina erityistä tarvetta eri asevoimien toiminnan tarkkailuun, koska joukkoja yleensä keskitetään lähelle eri valtioiden maarajoja (Kofman, 2021; National Post, 2017). Viimeisenä esimerkkinä mainittakoon sotilaalliseen toimintaan liittyneiden GPS-signaalien häiritsemistapaukset Barentsinmeren sekä pohjoisen Norjan alueella, joka ei pelkästään heikennä sotilaallista turvallisuusympäristöä, vaan aiheuttaa laajalti haittaa yhteiskunnalliselle toiminnalle, kuten kaupalliselle ilmailulle (Nilsen, 2017).

Edettäessä kuviossa myötöpäivään, seuraava hybridiuhkatekijä on *painostus ja uhkaaminen*. Sulkeisiin on täsmennetty muun muassa taloudellinen, poliittinen ja sotilaallinen kyseisen toiminnan vaikutusväylät, mutta kokonaisuudessaan tässä tarkoitettua painostavaa ja uhkaavaa käytöstä voi toteuttaa kaikissa niissä osa-alueissa, joissa valtiotasoiset tekijät toteuttavat keskinäistä kanssakäyntiä (valtiollisen tason toiminnan keinovalikoimaa voi kuvata mm. DIMEFIL ja PMESII -käsitteillä; ks. esim. Rodriguez, Walton & Chu, 2020). Uhkatekijän mukaisia toiminnan keinoja on muun muassa aggressiivinen voimapolitiittinen retoriikka, joka voi olla yhtä aikaa sekä poliittiseen tavoitteeseen painostamista että sotilaallisella voimalla uhkaamista. Esimerkkinä tästä voi pitää Euroopan Unionin huolestunutta kokemusta Venäjän käyttämästä retoriikasta. Vuonna 2019 Euroopan parlamentti antoi päätöslauselman siitä, että EU:n kokemuksen mukaan Venäjä osoittaa käytännössä olevansa halukas ja valmis käyttämään asevoimiaan, mukaan lukien ydinaseitaan, muita maita vastaan (Euroopan parlamentti, 2019). Painostus voi olla myös taloudellista, jota vaikuttamiskeinoa on käsitelty muun muassa Krimin miehityksen johdosta länsimaiden Venäjää kohtaan asettamien pakotteiden kautta (Mikkola, Aaltola, Wigell, Juntunen & Vihma, 2018, s. 39–48). Puhtaan poliittista painostusta, ilman sotilaallista näkökulmaa, on kuvattu tapahtuneen muun muassa Fennovoima-ydinvoimalahankkeen hyväksymisprosessissa vuonna 2015, jolloin vasta Suomen valtion enemmistöomisteisen energiayhtiö Fortumin vastahakoisesti tapahtunut mukaantulo voimalahankkeen rahoittajaksi varmisti hankkeen toteuttamiseksi edellytetyn tason länsimaisesta omistuspohjasta (Pynnöniemi & Saari, 2017).

Seuraavana uhkatekijänä on *jakolinjojen ja eripuraisuuden luonti*. Yhteiskunnallisella tarkastelutasolla, joka tässä on kyseessä, tämä tarkoittaa tutkimusaineiston perusteella kansallisen tarinan vääristelyä ja uudelleenkerrota, eli kansakuntaa yhdistävän historian ja yhteisen kokemuksen murentamista (esim. Valtioneuvosto, 2020, s. 12). Kansallista eripuraisuutta voi syntyä myös muutenkin kuin tavoittelisesta oman, mahdollisesti valheellisen, narratiivin kertomisesta ja levittämisestä. Muita kansakuntaa jakavia tekijöitä ovat kansalaisten kokemus epävakaa tai epätasa-arvoisesta yhteiskunnasta, jotka kokemukset lisäävät erilaisten ääriliikkeiden vetovoimaa sekä näiden liikkeiden keskinäisiä kiistoja ja yhteenottoja (Sisäministeriö, 2016, s. 17). Edelleen tällaisten ääriäkemyksiä ja tarkoituksellista provokaatiota synnyttävien liikkeiden tai aatteiden tavoitteellinen tukeminen, kuten rahoittaminen, voi sisältyä tähän

uhkatekijäluokkaan, mikäli siis sillä tukemisella pyritään uhkatekijän nimen mukaiseen vaikutukseen. Myös globaalit ilmiöt, kuten varallisuuden epätasainen jakautuminen, voi tutkimusaineiston mukaan luoda välillisesti kansallisiakin jakolinjoja, mikäli nämä globaalit haasteet aiheuttavat laajamittaista pakolaisuutta ja maahantuloa (Sisäministeriö, 2019a, s. 32). Mikäli tämä uhkatekijä olisi käsittänyt vain narratiivin kerronan, olisi sitä ollut haastava erottaa informaatiovaikuttamisen uhkatekijästä.

Omaksi uhkatekijäkseen erotettiin edellisestä tekijästä *demokraattisten rakenteiden horjuttaminen ja vaalivaikuttaminen*. Tällainen toiminta voi luoda kansakuntaan keskinäistä eripuraa ja kiihdyttää ääriliikkeiden toisiaan vastaan kohdistamaa vihamielistä toimintaa, mutta tämä esiintyi kuitenkin tutkimusaineistossa niin paljolti erillään edellisen uhkatekijän mukaisesta toiminnasta, että sen myötä se tuli tähänkin erottaa omaksi tekijäkseen. Esimerkiksi ulko- ja turvallisuuspoliittisessa selonteossa korostetaan että teknologisen kehityksen, kuten sosiaalinen media, myötä on mahdollistunut juuri tämänkaltaisia erityisiä vaikutusmahdollisuuksia (Valtioneuvosto, 2020, s. 15). Myös hallitusohjelmassa tunnistettiin että tämän aikakauden yksi keskeinen yhteiskunnallinen haaste on se, kuinka ylläpidetään kansalaisten luottamusta yhteiskuntarakenteisiin (Valtioneuvosto, 2019, s. 76).

Ensimmäisessä uhkatekijässä, ennustamattoman ja epävarman turvallisuusympäristön luonnissa, sivuttiin jo tätä seuraavaa uhkatekijää, *kriisitilanteiden luomista tai hyöäksikäyttöä*. Monessa kohtaa tutkimusaineistoja esiintyi turvallisuushuolena tai suoranaishana uhkana laajamittainen maahantulo sekä hallitsemattomat muuttoliikkeet (esim. Sisäministeriö, 2019a, s. 32), joka toimii hyvänä esimerkkinä tähän uhkatekijään. Erityisen hyvässä kansallisessa muistissa on vuoden 2015-16 talvella Venäjän kautta Suomeen tapahtunut turvapaikanhakija-aalto, joka tapauksena mainitaan sisäisen turvallisuuden selonteossakin (Sisäministeriö, 2016, s. 18). Samaan kategoriaan voi lukea Valko-Venäjän vuonna 2021 aloittamat pakolaisliikehdintää kiihdyttävät toimet, joissa se valtiojohtoisesti kuljettaa pakolaisia EU:n ulkorajoille, hakemaan turvapaikkaa eri jäsenvaltioista (Hiltunen, 2021). Myös valheellisen tiedon levittämällä voi aiheuttaa kohdeyhteiskunnassa kriisejä tai ainakin laajoja kiistoja, josta toiminnasta esimerkkinä voi mainita 2010-luvulla useasti esiin tuodut väitteet, että Suomessa ja muuallakin pohjoismaissa kaltoinkohdellaan lastensuojeluviranomaisten toimesta venäläistaustaisia lapsia (ks. esim. Lehmus 2010, Eerola 2014). Myös piilevää, mutta olemassa olevaa, potentiaalista kriisinaihetta voi kärjistää varsinaiseksi kriisiksi, kuten toteuttaa jo valmiiksi niukkojen energiavarantojen keinotekoista säätelyä. Asiasta on käytetty jopa energiaturvallisuus -käsitettä liittyen tapauksiin, joissa Venäjä on katkaissut maakaasutoimitukset Ukraina 2000-luvulla muutamaankin eri otteeseen (Bartuška, Lang & Nosko, 2019).

Informaatiovaikuttaminen on seuraava uhkatekijä edettäessä edelleen kuvioita myötäpäivään. Kyseessä on uhkatekijä, joka esiintyy varsin laajasti tutkimusaineistossa, sillä se on kaikissa muissa dokumenteissa mainittu, paitsi hallitusohjelmassa. Osassa tutkimusaineistoja se on pelkästään terminä esillä samalla

kerrotaan, että informaatiovaikuttaminen on osa hybridiuhkia (Sisäministeriö, 2016, s. 18). Mutta useimmissa selonteissa informaatiovaikuttamista määritetään, mitä sillä tarkoitetaan yhteiskunnallisella tarkastelutasolla. Kansallisessa riskiarviossa kerrotaan, että tässä toiminnassa tavoitteena on luoda kohdealueelle epävakautta tai vaikeuttaa päätöksentekoa muun muassa syöttämällä medialle vääristeltyjä tietoja (Sisäministeriö, 2019a, s. 28). Epävakauden luomiseksi voi käsittää ulko- ja turvallisuuspoliittisessa selonteossa mainitun informaatiovaikuttamisen tavoitteen ”yhteiskunnallisen keskustelun tarkoitushakuinen vääristäminen” (Valtioneuvosto, 2020, s. 15). Eli yhtenä tarkoituksena informaatiovaikuttamisessa on yhteiskunnallisella tasolla saada riittävä joukko kansalaisia kyseenalaistamaan poliittisten päätöksentekijöiden toimia, jolloin poliittinen liikkumavara kapenee. Toisena tarkoituksena on vaikuttaa itse päätöksentekoperusteisiin sumentamalla tosiasiallista faktatietoa ja tilannekuvaa reaali maailmasta. Esimerkkejä informaatiovaikuttamisesta nähtiin muun muassa Venäjän toteuttaman Krimin miehityksen yhteydessä vuonna 2014, jolloin Venäjän viralliset narratiivit sekä presidentin lausunnot kiistivät minkään miehitykseen liittyvän toiminnan olevan Venäjän toteuttamaa. Näillä toimilla arvioidaan olleen tavoitteena sekä Ukrainan että länsiyhteisön poliittisen päätöksenteon hidastuttaminen liittyen mahdollisiin vastatoimiin (Moore, 2019, s. 6). Myös vuoden 2016 Yhdysvaltain presidenttivaaleihin liittyvää vääristelevää ja suoraan valheellista uutisointia on tutkittu laajalti (ks. esim. Allcott & Gentzkow, 2017; Georgacopoulos & Mores, 2020). Tällaisella uutisoinnilla on joko mustamaalattu vastaehdokasta, tai suosittu omaa ehdokasta, ja sitä kautta tavoitteena on ollut saada oman ehdokkaan vaalisuosiota korotettua. Tutkimukset eivät aukottomasti pysty osoittamaan mikä tämän informaatiovaikuttamisen tuloksellisuus oli, mutta joka tapauksessa se on nykytiedon valossa kiistatonta, että tällaista vaikuttamista tapahtui (esim. Fujiwara, Müller & Schwarz, 2020).

Viimeisenä uhkatekijänä on *kybervaikuttaminen*. Tämä oli tutkimusaineistossa kaikista laajimmin esiintynyt hybridiuhka, sillä se oli mainittu jokaisessa dokumentissa. Kybervaikuttamisesta puhutaan kasvavana ja monipuolistuvana uhkavektorina (Valtioneuvosto, 2017, s. 9; Valtioneuvosto, 2020, s. 17), jolloin halutaan korostaa kyseisen vaikuttamiskeinon muuttuvaa ja laajentuvaa luonnetta. Kybervaikuttamisen kohteena nähdään tutkimusaineiston perusteella olevan ainakin kriittisen infrastruktuurin toimijat, teollisuuslaitokset sekä yhteiskunnan elintärkeiden toimintojen mukaisia toimialoja (Valtioneuvosto, 2017, s. 9; Sisäministeriö, 2016, s. 41–52). Mikäli tarkastelee kansallisen tietoturvanomaisen, eli Kyberturvallisuuskeskuksen, raportteja kuluneen vuoden merkittävistä kyber- ja tietoturvapoikkeamista (kuukausittaiset Kybersäätiedotteet), voi havaita, että vakavin tilanne muodostuu kansalaisiin kohdistuvista tietojenkalastelu- ja huijausviesteistä. Koko vuoden ajan tilanne näiden viestien ja huijausten suhteen on ollut joko huolestuttava tai vakava, jotka ovat Kybersäätiedotteiden luokitteluasteikon kaksi vakavinta luokkaa. Toki kaikki tällainen toiminta ei ole tavoitteellista yhteiskuntaamme kohdistuvaa hybridivaikuttamista, mutta yksittäisiin kansalaisiin kohdistuva ja alati voimistuva digitaalinen huijaustoiminta voi lopulta muodostaa luottamuspulaa myös yhteiskuntaa koh-

taan, eikä pelkästään luottamuspulaa sitä palveluntarjoajaa kohtaan, jonka nimissä huijauksia tehdään. Hallitusohjelma tunnistaakin tarpeen kasvattaa kansalaisten kyberosaamista (Valtioneuvosto, 2019, s. 80). Tapahtumia, jotka voidaan luokitella tämän tutkielman mukaiseen hybridiuhkien kybervaikuttamiseen, on muun muassa Venäjän toteuttamat tietoverkkohyökkäykset Ukrainan valtion ja yhteiskunnan eri osiin, ja todennäköisesti kuuluisimpana näistä vuoden 2015 hyökkäys Ukrainan sähköverkkoyhtiöihin (Cerulus, 2019). Myös kolsi muita kyberhyökkäyksiä tapahtuu taukoamattomalla tahdilla, ja joista merkittävä osa nimetään valtiollisten toimijoiden toteuttamaksi, jolloin näiden vaikuttamismekanismien motivaattorina on mahdollisesti valtiolliset tavoitteet (ks. esim. CSIS, 2021).

Viimeisenä on syytä korostaa, että hybridiuhkien luonteeseen kuuluu eri vaikutusmekanismien yhdenaikainen sekä keskenään suunniteltu ja koordinoitu käyttö (Limnell & Iloniemi, 2018, s. 22). Vaikka uhkatekijät ovat visuaaliseen kuvioon eroteltu omiin laatikkoihin, niiden kuvauksissa pyrittiin uhkatekijän konkretisoimisen lisäksi näyttämään niiden keskinäisriippuvuutta; informaatiovaikuttamisen kuvauksessa kerrottiin Yhdysvaltain vaalikampajaan vaikuttamisesta, ja vaalivaikuttaminen on myös osa toistahybridiuhkatekijää. Tai voimakas kybervaikuttaminen yhteiskunnan tietojärjestelmäninfrastruktuureihin voi myös samalla toimia painostuskeinona sekä luoda kriisitilanteita. Seuraavaksi vertaillaan muodostettua hybridiuhkakäsitettä tiedustelulakeihin.

4 TUTKIMUSTULOKSET

Tässä pääluvussa muodostetaan koodatun tutkimusaineiston perusteella tutkimuksen tulokset, eli päätutkimuskysymykseen vastaus. Pääluku alkaa alaluvulla, jossa vertaillaan muodostettua hybridiuhkakäsitettä tiedustelulakeihin. Tässä vertailussa tiedustelulakeja tulkitaan samalla ankkuroiden menetelmän mukaisella tutkimusotteella kuin itse tutkimusaineistoakin, eli vain tekstissä olevat asiat otetaan huomioon – ja ne otetaan huomioon sellaisenaan, ilman olettamuksia ja johtopäätöksiä. Vertailun tarkoituksena on etsiä vastausta kysymykseen, kuinka hyvin tiedustelulakien suomilla tiedonhankintamandaateilla voidaan vastata hybridiuhkiin?

Vertailun jälkeen esitetään omassa alaluvussa sen myötä syntyvät tutkimustulokset. Erikseen omassa alaluvussa avataan erästä huomioita, joka tuli ilmi tutkimus- ja lähdeaineistoja tarkastellessa. Kyseessä on teksteissä esiintynyt tapa, että informaatio- ja kybervaikuttamista käsitellään monessa kohtaa yhtäaikaisesti ja yhdessä, jossa ei sinänsä ole ongelmaa. Mutta erityisesti on syytä kiinnittää huomiota siihen, että informaatiovaikuttaminen näyttäisi monesti saavan perusteettomasti kybervaikuttamista pienemmän roolin ja painoarvon.

Pääluvun päättää katsaus aihealueen aiempaan tutkimukseen. Samalla myös nyt tässä tutkimuksessa saatuja tuloksia vertaillaan aiempiin tutkimustuloksiin. Sen avulla nähdään, ovatko eri tutkimusten tulokset keskenään ristiriidassa, vai vahvistaako saadut tulokset toisiaan.

4.1 Hybridiuhkien vertailu tiedustelulakeihin

Tämä vertailu aloitettiin tarkastelemalla hallituksen esityksiä sotilas- ja siviilitiedustelulaeista (HE 202/2017 sekä HE 203/2017). Nämä esitykset sisältävät siis itse lakitekstiehdotuksen ohessa silloisen nykytilan kuvauksen, perustelut lakitarpeesta, sekä arvion lain vaikutuksista.

Kybervaikuttamisen uhkatekijä esiintyy varsin laajasti molemmissa hallituksen esityksissä. Kyber sanana tai yhdyssanan osana esiintyy siviilitiedustelulakiesityksessä 96 kertaa, eli keskimäärin noin joka neljännellä sivulla. Sotilastiedustelun lakiesityksessä esiintymismäärä on 86 kertaa, ja sivumäärän esityksessä ollessa melkein sama, esiintymistiheys on yhtäläinen. Kybervaikuttamisen uhka nähdään tiedustelulaeissa olevan muun muassa kybertoimintaympäristössä tapahtuvaa vakoilua, joka on erityisluonteista siksi, että se voi jatkua huomaamattomana jopa vuosia sekä kiinnijäämisen riski on ylipäätään alhainen (HE 203/2017, s. 11). Itse tiedustelu- tai vakoiluohjelmien lisäksi kohdetietojärjestelmiin voidaan toimittaa tarvittaessa aktivoitavia haittaohjelmia, joilla siis pyritään eri tavoitteisiin kuin tietoa keräävillä ja lähettävillä tiedusteluohjelmilla (HE 203/2017, s. 11). Lakiesityksessä mainitaan Suomen kyberturvallisuustapahtumien havainnointikyvyn olevan puuttellinen, ja että tiedustelulaeilla tätä puutetta pystytään paikkaamaan.

Konkreettisina kohtina tiedustelulaeissa esitöineen kyberuhkien torjumiseen mainitaan lain sähköisen viestinnän palveluista (917/2014) pykälä 272 §, jossa määrätään toimenpiteet tietoturvan toteuttamiseksi (HE 203/2017, s. 44). Viittaus tehdään myös julkisen hallinnon turvallisuusverkkotoiminnasta annettuun lakiin (10/2015), jonka tarkoituksena mainitaan olevan muun muassa se, että valtion johtaminen ja keskeisten viranomaisten toiminta mahdollistuu kaikissa yhteiskunnallisissa oloissa (HE 203/2017, s. 45). Itse tiedustelulaeissa tulee myös valtuuksia vastata haitallisiin kybertoimiin sillä vastuulla, että siviilitiedusteluviranomaisella Suojelupoliisilla on kyky hankkia tarvittava kyberuhkia koskevan tiedustelutiedon kansainvälisellä yhteistyöllä, ja sotilastiedustelulla on kyky toteuttaa uhkia torjuva tietoliikennetiedustelu teknisellä tasolla, myös omien kansainvälisten yhteistyösuhteiden lisäksi (HE 203/2017, s. 136). Tällöin, kun tiedustelutiedon perusteella on osoitettavissa tarve tietoliikennetiedustelulle, ohjataan viestintäverkosta osoitetun ja rajatun kohdan tietoliikenne Puolustusvoimien tiedustelulaitokselle (laki sotilastiedustelusta 590/2019, 68–72 §). Kun lakiesityksessä viitattiin myös uhkatoimijan mahdollisuuteen asentaa nukkuvia haittaohjelmia, myös tähän on otettu kantaa laissa sotilastiedustelusta. Mikäli tietoliikennetiedustelussa saadaan havaintoja haittaohjelmasta, kyseiset tiedot voidaan luovuttaa eteenpäin sille taholle, jota asia koskee, mikäli se on haittaohjelman kohteen tai yleisen turvallisuuden taikka maanpuolustuksen kannalta edellytettävää (laki sotilastiedustelusta 590/2019, 74 §; laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019, 16 §).

Tarkastellaan tutkimusaineistossa toiseksi eniten esiintynyttä hybridiuhkatekijää, *informaatiovaikuttamista* (kybervaikuttaminen oli siis laajimmin esiintynyt). Myös tämä uhka esiintyy hallituksen esityksissä molempien lakien kohdalla. Kirjausmuoto nykytilan kuvauksessa on paljon puhuva: informaatiovaikuttamista on kohdistettu sekä Suomeen että lähialueillemme muun muassa poliittista päätöksentekoa sekä kansalaisia vastaan. Informaatiovaikuttaminen on tunnistettava ja siihen on pystyttävä vastaamaan. (HE 202/2017, s. 9; HE 203/2017, s. 7–8)

Muutoin informaatiovaikuttaminen ei esiinny kuin yksittäisiä kertoja turvallisuusympäristön nykytilan kuvauksessa tai muussa itse tiedustelulakeja taustoittavassa tekstissä, joten esiintyvyys on lopulta vain muutamia prosentteja verrattuna kybervaikuttamiseen. Joka tapauksessa informaatiovaikuttamiseen vastaamiseksi on otettu kantaa itse tiedustelulaeissa. Siviilitiedustelun laillisista kohteista määräävä pykälä (poliisilaki 872/2011, 5 a luku 3 §) antaa tiedustelutoimivallan myös havaittua tai perustellusti oletettua informaatiovaikuttamistoimintaa vastaan. Kyseisen pykälän 7. kohta tarkoittaa sellaista laillista siviilitiedustelun kohdetta, jossa kohteena on vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille. Tämän lainkohdan perusteluissa kerrotaan, että vieras valtio voi käyttää vihamieliseen toimintaan laajaa keinovalikoimaa, johon kuuluu myös informaatiovaikuttaminen. Tätä vaikuttamista voi kyseinen taho pyrkiä toteuttamaan siten, että se tarkoituksellisesti haluaa peitellä omaa toimintaa. Tällöin kohdevaltio ei välttämättä voi tietää, onko kyseessä vieraan valtion tavoitteellinen operaatio vai ei. Tämän lainkohdan myötä voidaan käyttää tiedustelumenetelmiä tiedon hankkimiseksi tällaisesta informaatiovaikuttamistoiminnasta, kuten myös tällaisen toiminnan valmisteluista. (HE 202/2017, s. 175)

Myös sotilastiedustelussa annetaan tiedustelumenetelmien toimeenpanon mandaatti informaatiovaikuttamisen tapauksissa, myös siinä vaiheessa mikäli on viitteitä sellaisen toiminnan valmisteluista (laki sotilastiedustelusta 590/2019, 4 §:n 1. mom:n 1. kohta; HE 203/2017, s. 185). Ja ero sotilas- ja siviilitiedustelun toimivallan välillä tulee siitä, että vaikka sotilastiedustelussa voidaan yhtä lailla hankkia tietoa Suomeen kohdistuvasta informaatiovaikuttamisesta, mutta tarkoitus on siinä, että samalla selvitetään, onko kyseisen toiminnan takana myös sotilaallisia pyrkimyksiä (HE 203/2017, s. 185).

Kuten jo edellisluvussa hybridivaikuttamisen käsittekarttaa eritellessä kävi ilmi, monet uhkatekijät lomittuvat päällekkäin, kuten vaalivaikuttaminen toimintana voi olla esimerkiksi sekä demokraattisten rakenteiden horjuttamista että kansakunnan eripuraisuuden luontia. Näin myös seuraavia uhkatekijöitä on loogista käsitellä yhtenä kokonaisuutena: *kriisitilanteiden luominen tai hyöäksikäyttö, demokraattisten rakenteiden horjuttaminen ja vaalivaikuttaminen sekä jakolinjojen ja eripuraisuuden luonti*. Yhtenä syynä tähän niputtamiseen on myös se, ettei näitä tekijöitä esiinny erikseen eriteltyinä tiedustelulaeissa, eikä myöskään hallituksen taustaesityksissä, vaan näitä teemoja käsitellään yhtenä kokonaisuutena, kuten seuraavaksi esitellään.

Siviilitiedustelupuolta ensiksi tarkastellessa on hyvä aloittaa siitä, että kaikki edellä lueteltu uhkatoiminta tulee olla niin voimakasta, että tiedusteluluvan antava taho (tuomioistuin, Suojelupoliisin päällikkö tai päällystään kuuluva poliisimies – päättävä taho riippuu minkä tiedustelumenetelmän käyttöön haetaan lupaa) voi todeta, että kyseinen toiminta uhkaa vakavasti kansallista turvallisuutta (poliisilaki 872/2011, 5 a luku 4 §). Uhkatoiminnan tapahtuminen tulee olla joko perustellusti oletettua tai todennetusti havaittua. Nämä ehdot pätevät yleisesti kaikkeen

siviilitiedustelutoimintaan. Sinäsa ei ole väliä sillä, onko toteuttava taho valtiollinen, ei-valtiollinen tai vaikka yksittäinen henkilö, vaan uhkan taso on määrittävä tekijä (HE 202/2017, s. 172).

Edellä informaatiovaikuttamista eritellessä esiteltiin jo lainkohta, jossa määrätään siviilitiedustelun kohteet. Samassa lainkohdassa yhdeksi tiedustelukohteeksi määritetään terrorismi (poliisilaki 872/2011, 5 a luku 3 § 1. kohta), ja lakiesityksessä terrorismi käsitteenä määritetään seuraavasti: toiminta, jonka tarkoituksena on pelotella vakavasti väestöä, horjuttaa vakavasti valtion sosiaalisia, poliittisia tai perustuslaillisia rakenteita (relevantit kohdat terrorismin määritelmästä peilaten nyt käsittelyssä oleviin uhkatekijöihin, HE 202/2017, s. 172). Eli tämä lainkohta antaa tiedustelutoiminnan mandaatin näihin uhkatekijöihin liittyen tai ainakin osaan mahdollisista uhkatoiminnan tapauksista. Erityisesti tällä lainkohdalla voidaan vastata uhkatekijään demokraattisten rakenteiden horjuttaminen.

Myös niissä tapauksissa, joissa viranomaiset joutuvat hoitamaan erilaisia kriisitilanteita, on tiedustelulaeissa tunnistettu tiedustelullinen tiedonhankinnan tarve. Sotilastiedustelulain esitöissä mainitaan tällaisissa tilanteissa tarve tiedonhankintaan Puolustusvoimia (HE 203/2017, s. 88). Erityishuomiona tähän uhkatekijöiden kategoriaan on mainittava se, että sotilastiedustelulaissa mainitaan, ettei Puolustusvoimat voi puuttua sellaisiin Suomen sisäisiin tapahtumiin, joissa kansalaiset omasta aloitteestaan synnyttävät valtion tai yhteiskunnan sisäisiä konflikteja – ja näissä taustalla ei siis ole vieraan valtion vaikuttamista tai tukea (HE 203/2017, s. 184). Tämä ulkoa päin tulevan uhkatoimijan edellytys on periytynyt lakitekstiin asti, ja tiedustelutoiminnan mandaatti sotilastiedustelulle erilaisissa kriisitilanteissa ja yhteiskunnan horjuttamistapauksissa tulee näillä reunaehdoilla lainkohdasta 590/2019 4 §:n 2. momentista. Siviilitiedustelulain esitöissä tämä sama uhkatekijöiden teema on ilmaistu huomattavasti laveammin, painottaen yleisesti tiedustelutiedon suurta merkitystä viranomaisten torjuessa kaikkia uusia uhkia. Tavoitteena siviilitiedustelulainsäädännöllä on tässä uhkatekijäkategoriassa siis se, että analysoitu tiedustelutieto koskien uusia uhkia on kaikkien turvallisuusviranomaisten sekä kansallisen turvallisuuden suojaamiseen osallistuvien toimijoiden käytössä oikea-aikaisesti (HE 202/2017, s. 8). Lakitekstiin tämä on periytynyt kahteen eri kohtaan (poliisilaki 872/2011, 5 a luku 3 §:n 5. ja 11. kohdat), joiden perusteella legitimoidaan tiedustelutoimet laillista yhteiskuntajärjestyksestä vakavasti uhkaavaa toimintaa kohtaan.

Viimeisinä uhkatekijöinä, joita ei ole vielä vertailtu, on *painostus ja uhkaaminen sekä ennustamattoman ja epävarman turvallisuusympäristön luonti*. Koska näissä molemmissa uhkatekijöissä toiminnan luonne on sellaista, jossa tekijän tulee eksplisiittisesti identifioitua, on niitä loogista vertailla yhdessä tiedustelulakeihin. Siis, kun monet muut uhkatekijät, kuten kybervaikuttaminen tai informaatiovaikuttaminen, on useasti luonteeltaan sellaista, että tekijä joko tarkoituksella joko piiloutuu, väärentää identiteettinsä tai käyttää kolmatta osapuolta toimintansa toteuttamiseen, on näille uhkatekijöille ominaista toiminnan toteuttajan identifioituminen. Uhkailun voi

toki esittää epäsuorasti tai piiloviestillä, mutta uhkauksen täytyy tulla varsinaiselta toimijalta – eihän se muutoin ole uhkaavaa toimintaa. Myös jos turvallisuusympäristöä horjuttava toiminta on piiloteltua ja salassa pidettävää, voiko kohde edes havaita tai käsittää turvallisuusympäristön horjumisen? Näin ollen näiden kahden uhkatekijän tarkastelu yhdessä on loogista, koska nyt voidaan tutkia tiedustelulakeja tarkastellen, millä tavalla se legitimoit tiedustelutoiminnan sellaista kansallista turvallisuutta vaarantavaa toimintaa kohtaan, jossa uhkan aiheuttajataho on lähtökohtaisesti tiedossa.

Sotilastiedustelulaissa annetaan selväsanaisesti toimivalta tiedustelulle niissä tapauksissa, jossa vieraan vallan asevoimat (sekä niihin rinnastuvat joukot) toteuttavat sotilaallista voimakäyttöä, valmistelevat sitä, ryhmittävät joukkoja tai toteuttavat tiedustelutoimintaa Suomen maanpuolustusta kohtaan (laki sotilastiedustelusta 590/2019, 4 § 1. mom:n 1. kohta). Edelleen lain esitöissä kirjoitetaan, että tämän kaltaisesta toiminnasta tietoa hankkimalla pyritään vähentämään epävarmuustekijöitä Suomen turvallisuusympäristöstä, joka tässä vertailutapauksessa vastaa käsittelyssä olevaan uhkatekijään. (HE 203/2017, s. 183–184)

Siviilitiedustelulainsäädännössä tämän kaltaiseen toimintaan otetaan kantaa siten, että lainsäädännön tulee mahdollistaa Suomen turvallisuusympäristön tilan ja kehityksen seurannan, eli tiedonhankinnan luonne voi tässä yhteydessä olla pitkäkestoista tai jatkuvaa (HE 202/2017, s. 74). Tämä vaatimus on siirtynyt lakitekstiin, kun tiedustelutoiminnan mandaatti tällaisessa skenaariossa tulee siviilitiedustelun kohteista terrorismi, sekä kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi (poliisilaki 872/2011, 5 a luku 3 §:n 1. ja 8. kohdat; HE 202/2017, s. 177). Painostukseen ja uhkaavaan toimintaan voi parhaiten nähdä vastattavan saman lainpykälän 5. kohdalla, joka antaa tiedustelumandaatin kansainvaltaista yhteiskuntajärjestystä vakavasti uhkaavaa toimintaa kohtaan. Lainkohdan perusteluissa tarkennetaan, mitä tällainen toiminta on, muun muassa esimerkillä ”toiminta, joka pakottaa hallitusvaltaa käyttäviä henkilöitä tekemään tai jättämään jotain tekemättä heidän valtiollisissa tehtävissään” (HE 202/2017, s. 174). Tämä vastaa siihen, mitä hybridiuhkien mukaisella painostamisella tai uhkaamisella halutaan saavuttaa.

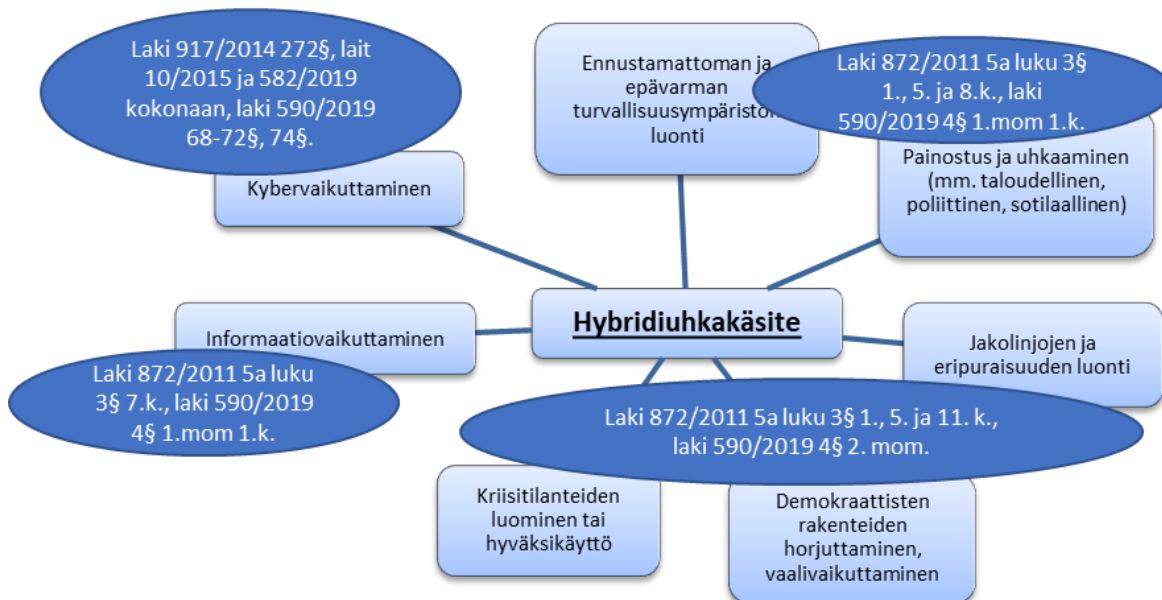
Sotilastiedustelulaissa painostukselliseen toimintaan vastaaminen on kirjoitettu hieman suoraviivaisemmin, sillä lain esitöissä mainitaan, että sotilastiedustelun kohteen voi olla sellainen toiminta, jolla pyritään vaikuttamaan valtionjohdon päätöksentekoon poliittisilla ja taloudellisilla painostuskeinoilla (HE 203/2017, s. 185). Tarkempia perusteluja annetaan sen suhteen, miksi sotilastiedustelulla saa hankkia tietoa valtionjohtoa koskettavista uhkista, jotka eivät suoraan ole Suomen maanpuolustukseen kohdistuvia uhkia: ”painostuskeinojen taustojen selvittämisen avulla on suora yhteys ennakkovaroituksen antamiseen sotilaallisen uhan kehittymisestä” (HE 203/2017, s. 185). Eli painostus valtiotamme kohtaan nähdään sellaisena keinona, mitä todennäköisesti käytetään yhdessä muiden keinojen kanssa, tai ennen muiden keinojen aloittamista. Tämä perustelu on kirjoitettu sotilastiedustelun laillisten kohteiden listassa kohtaan vieraan valtion asevoimien (ja niihin rinnastuvat toimijat) toiminta ja toiminnan

valmistelu (laki sotilastiedustelusta 590/2019, 4 §:n 1. mom:n 1. kohta), eli kyseinen lainkohta siis antaa tiedustelumandaatin sotilastiedustelulle hybridiuhkien painostus ja uhkaaminen -uhkatekijän mukaiseen toimintaan.

Esitellään seuraavaksi tämän vertailun myötä syntyvät tutkimustulokset.

4.2 Tutkimustulokset

Edellä tehty vertailu voidaan helposti esittää myös visuaalisesti, jolloin voidaan kuvan muodossa tiivistää tekstimuotoinen vertailu hybridiuhkien ja tiedustelulakien välillä (kuvio 4). Kuviossa on käytetty pohjalla kuvion 3 hybridiuhkakäsittekarttaa, jonka päälle on lisätty lainkohdat ellipsimäisiin kupliin siten, että ne leikkaavat niiden uhkatekijöiden päälle, joista kyseisellä lainkohdalla voidaan hankkia tiedustelutietoa. Vertailun perusteella voidaan lausua, että valtionhallinnon virallisista, kansallisia uhkakuviä käsittelevistä asiakirjoista muodostettuun hybridiuhkakäsitteeseen kyetään vastaamaan tiedustelulaeilla niiltä osin, mitä kyseisistä uhkatoiminnoista tai toiminnan valmisteluista tulee tietoa hankkia kansallisen turvallisuuden suojaamiseksi. Tämä ei tietenkään tarkoita sitä, että kaikesta hybridiuhkien kenttään menevästä toiminnasta tieto tiedusteluviranomaisilla olisi, vaan pikemminkin tarkoittaa sitä, että tiedustelulait eivät ainakaan estä tiedonhankintaa hybridiuhkien eri uhkakategorioista.



KUVIO 4. Hybridiuhkakäsite vertailtuna tiedustelulakeihin.

Tutkimuksen perusteella voidaan lausua päätutkimuskysymykseen vastauksena, että nykymuotoisilla tiedustelulaeilla voidaan vastata nykymuotoisiin hybridiuhkiin siten, kuin hybridiuhkat suomalaisessa kontekstissa käsitetään. Tiedustelulait voivat jättää aukkoja yksittäisten ja spesifien uhkien torjuntaan, siis yksittäisten tapausten paljastamiseen tai ennakkovaroittamiseen. Mutta itse hybridiuhkakäsitteen ylätasoa vaikuttamismekanismista, eli tämän tutkielman hybridiuhkakäsittekartan avainkategorioista, on mahdollista hankkia tietoa kansallisen turvallisuuden säilyttämiseksi.

Tiedustelulakien sisällä, tiedustelun kohteista määrävissä lainkohdissa (laki sotilastiedustelusta 590/2019, 4 § ja poliisilaki 872/2011, 5 a luku 3 §) ei ole sorruttu liian spesifiin määrittelyyn sen suhteen, minkälaisesta toiminnasta saa tiedustelutietoa hankkia. Tämä laava ote uhkien määrittelyissä sopii hyvin hybridiuhkien muuttuvaan luonteeseen, sillä Suojelupoliisikin on hybridiuhkia kuvannut siten, että siihen kuuluu ”muuta, tarkemmin määrittelemättömiä toimia” (ks. kuvio 1).

Tutkielman apukysymyksiä on asetettu kaksi kappaletta, joista ensimmäinen kysyy mitä hybridiuhkat ovat, ja toinen, että mitä lakeja tiedustelulakikonaisuus käsittää sekä kuinka viranomaisoimivaltuudet muuttuivat verrattuna aikaan ennen tiedustelulakeja. Hybridiuhkat ovat selkeä kertoa visuaalisessa muodossa, eikä tekstinä tähän kirjoitettuna, joten ensimmäiseen apukysymykseen vastauksen näkee kuvioista 3. Toinen apukysymys on purettu osiin ja vastattu pääluvun 2 sisällä, sekä tiedustelulait ovat kerrottu luvussa 2.2. Yhteenvedon toisen apukysymyksen osalta sen suhteen, mitä toimivaltuusmuutoksia tiedustelulait toivat, niin vastaus siihen on kaksiosainen, jakautuen sotilas- ja siviilitiedusteluun. Sotilastiedustelun osalta saatiin ensikertaa varsinaisesti säädettyä toimivaltuudet tiedonhankintaan, jolloin sotilastiedustelun ei enää tarvinnut hankkia tietoa pelkästään rikosperusteisilla toimivaltuuksilla, tai viraston sisäisillä normeilla, tai olla muuten toimivaltuuksien osalta puutteellisessa tilassa. Siviilitiedustelun osalta tilanne oli siinä mielessä verrattavissa sotilastiedusteluun, että ennen nykymuotoisia tiedustelulakeja tiedustelullisia tai tiedonhankinnallisia toimivaltuuksia ei ollut määrätty, jos viranomainen halusi hankkia tietoa etupainoisesti kansallista turvallisuutta horjuttavista uhkista. Toimivaltuus tiedonhankintaan tuli siis siviilipuolellakin rikostorjunnallisesta tavoitteesta, piti siis olla syy olettaa rikoksen jo tapahtuneen tai tapahtuvan. Samalla tiedustelun kohteelle oli asetettu muitakin vaatimuksia, kuten että sen tuli sijaita Suomen valtion alueella. Tiedustelulakien yhteydessä siviilitiedustelua toteuttavalta viranomaiselta, Suojelupoliisilta poistettiin esitutkintaviranomaisen asema, ja näissä laeissa sille annettiin toimivalta hankkia tietoa ilman rikosepäilyperustetta. Myös tehtävä rikoksia tutkivasta organisaatiosta poistettiin. Tiedustelulait siis kaiken kaikkiaan mahdollistivat tiedustelupalveluidemme todellisen muotoutumisen, poliisiorganisaatiosta kohti siviilitiedustelupalvelua, ja rikostorjunnallisesta sotilastiedusteluorganisaatiosta kohti sotilastiedustelupalvelua.

4.3 Keskeisiä havaintoja hybridiuhkien ja tiedustelulakien vertailusta

Tässä luvussa nostetaan esiin keskeisiä havaintoja, joita syntyi tiedustelulakien, niihin liittyvien hallituksen lakiesityksien ja hybridiuhkien välisessä vertailussa. Tässä edellisluvussa tehdyssä vertailussa pääkysymys oli siis, voiko tiedustelulaeilla vastata tehokkaasti jokaiseen uhkatekijään?

Viimeaikoina, ja edelleenkin merkittävästi esillä ja julkisessa keskustelussa näistä uhkatekijöistä on kyber- sekä informaatiovaikuttaminen. Esimerkiksi vuonna 2019 Valtioneuvoston kanslia ohjasi tutkimusrahaa informaatiovaikuttamisen tutkimiseen osin juuri siksi, että kyseinen toiminta on saanut osakseen niin paljon huomiota (Lankinen, 2018, s. 98) ja kybervaikuttamisen jokapäiväisyydestä on lähihistoriassa toistettu monissa eri julkisissa puheissa tai lausunnoissa (Kaikkonen, 2021; Pulkkinen, 2017).

Kybervaikuttamiseen otettiin hallituksen esityksissä kantaa varsin mittavasti, verrattuna muihin uhkatekijöihin. Kybervaikuttaminen esiintyi läpi hallitusten esitysten, ja sen merkitystä korostettiin monessa kohdin. Tämä näkyikin annetuissa toimivaltuusmandaateissa, sillä kybervaikuttamiseen vastaamiseksi on monta eri lainkohtaa, ja itse lakejakin, jotka antavat toiminnan mandaatin.

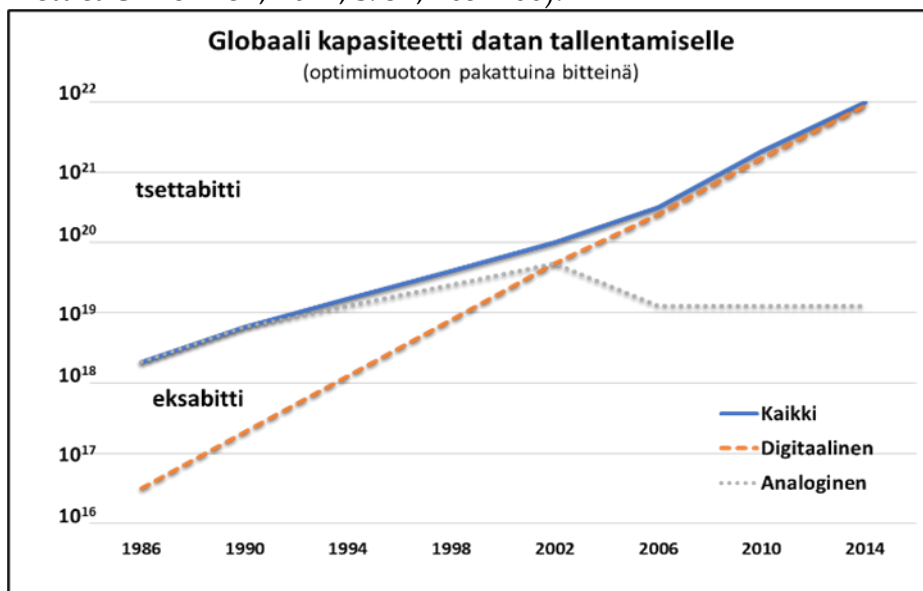
Informaatiovaikuttaminen taasen näyttäytyy eri tavalla mielenkiintoisena uhkatekijänä siinä suhteessa, että vaikka sekin esiintyy laajasti, siihen vastaaminen ei näyttäydy yhtä yksiselitteisenä. Kuten luvun 4.1 hybridiuhkien ja tiedustelulakien välisessä vertailussa esiteltiin, laillisissa tiedustelun kohteissa on kyllä tunnistettu informaatiovaikuttaminen, mutta esimerkiksi Suojelupoliisin johtaja on nostanut esiin tiedustelulakien aukkoja (Pietiläinen, 2021). Ilmeisesti lakipuutteet tai -aukot eivät kuitenkaan ole kansallista turvallisuutta vaarantavia, sillä Suojelupoliisi ei ole vaatimassa lisätoimivaltuuksia, vaan nämä seikat ovat tuotu julki siksi, että Suojelupoliisilta on tätä lakiarviointia pyydetty (Rantala, 2021). Yhtä kaikki siinä yhteydessä Suojelupoliisin johtaja mainitsee, että kansallista turvallisuutta uhkaava toiminta voidaan helposti siirtää vaikkapa kotirauhan suojaamaan paikkaan, jolloin perustuslaki turvaa kyseisen tilan koskemattomuuden tiedustelutoiminnalta. Nyt, kuten tässä tutkielmassa on osoitettu, hybridiuhkien luonteeseen kuuluu useiden eri vaikuttamiskeinojen joustava käyttö, ja monin paikoin vielä oman toiminnan peittäminen, ei liene perusteltua informaatiovaikuttamisen yhteydessä olettaa, että toiminta tapahtuisi aina sellaisesta lokaatiosta, johon tiedustelulait antavat tiedonhankinnan valtuuden. Varsinkin nyt enää, kun tämä perustuslain voima kotirauhan yhteydessä on nostettu selväsanaisesti julkiseen keskusteluun ja tietoisuuteen.

Muutoinkin, kun informaatiovaikuttamista käsitellään hallituksen lakiesityksissä useassa kohtaa yhdessä kybervaikuttamisen kanssa, monessa tällaisessa kohdassa teksti jatkuu kuitenkin kertomalla vain tarpeesta kyberpuolustuskyvyn kehittämiseksi, tai korostaen kykyä

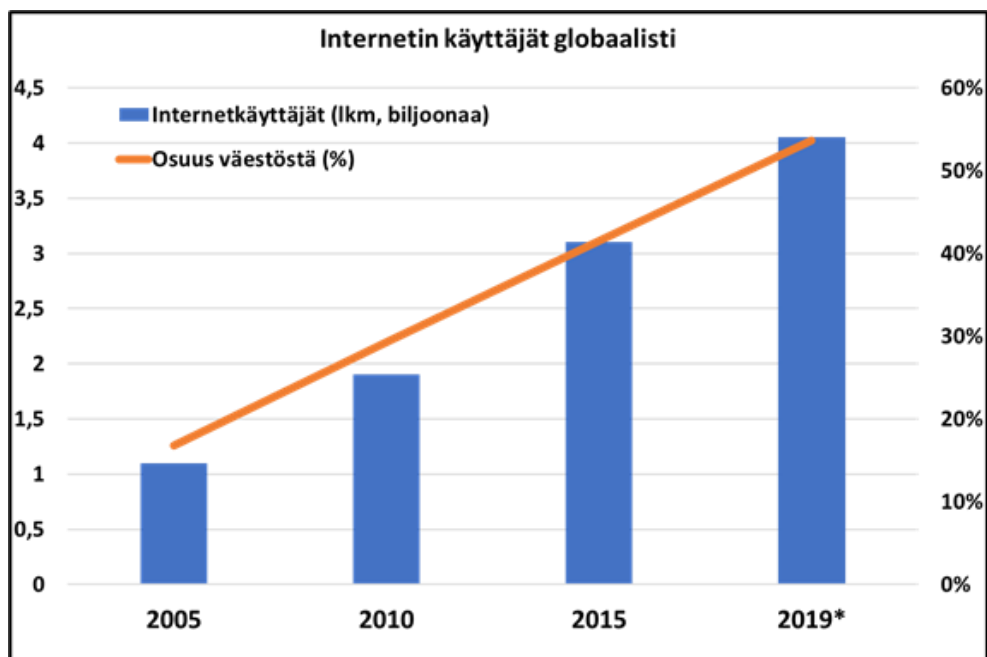
kybertoimintaympäristössä toimimiseen (ks. esim. HE 203/2017, s. 7). Informaatiovaikuttaminen ei tässä kohdin näyttele oikeastaan ollenkaan roolia, vaikka tiedon käyttäminen toiseen ihmiseen vaikuttamiseen on toimintana yhtä vanhaa kuin ylipäättään ihmisten välinen kommunikaatio (Harari, 2011, s. 30–31). Jotta voidaan perustellusti lausua informaatiovaikuttamisen uhkapotentiaalista kansallista turvallisuutta kohtaan, tulee tämän tyyppistä vaikuttamista tarkastella kokonaisvaltaisesti – mukaan lukien sen historiallista kehitystä.

Ihmiskunnan historiaa tutkittaessa on huomattu useita tuottavuuden kehitysloikkia, joita kutsutaan vallankumouksiksi. Tutuimmat vallankumoukset lienevät viime vuosisadoilla tapahtuneet teolliset vallankumoukset, mutta kun sieltä kuljetaan ajallisesti kohti nykyhetkeä, on tapahtunut muitakin vallankumouksia. Tuorein yleisesti hyväksytty vallankumous on informaatio- ja kommunikaatioteknologian tuoma vallankumous (ks. esim. Rifkin 2011), ja vaikka sitä käsitellään monissa yhteyksissä nimenomaan taloudellisesta näkökulmasta, niin taustalla kyseessä on kuitenkin digitaalisen tiedon virran syntymisestä ja sen hyväksikäytöstä – välinearvosta – jotain muuta tarkoitusta varten.

Vaikka vasta tämä viimeisin vallankumous kuvastaa tiedon ja sen välittämisen suurta merkitystä, on nykyajan tiedolla vaikuttamisen ilmiö tunnistettu esiintyvän jo antiikin ajalla (ks. mm. Pitkänen & Sutinen, 2018). Ilmiötä kuvaava termi on vaihdellut aikojen saatossa, ja tällä hetkellä käytössä olevan termi informaatiovaikuttaminen alakäsitteineen ovat varsin tuoreita. Muun muassa *vaihtoehtoiset totuudet* -alakäsite lanseerattiin vuonna 2017 Yhdysvaltain presidentti Trumpin kabinetin toimesta (Sinderbrand, 2017). Toinen tunnettu tiedolla vaikuttamisen ilmiötä kuvaava termi on *propaganda*, jota käytetään kuvaamaan erityisesti tapahtumia viimevuosisadalla, painottuen ensimmäisen ja toisen maailmansodan aikaisiin tiedolla vaikuttamisen operaatioihin. Myös kyseisten ajanjaksojen tieteellisessä tutkimuksessa propagandatermi esiintyi laajalti, mutta toisen maailmansodan jälkeen aihealueen tutkimuskentässä tapahtui terminologinen siirtymä propagandasta kohti suostuttelua, tai taivuttelua (*persuasion*), joka jo kuvastaa nykyhetken ajattelutapaa, eli tietoa käytetään välineenä, jonka avulla saadaan toinen ihminen tekemään vapaaehtoisesti jotain (Jowett & O'Donnell, 2012, s. 32, 165–166).



KUVIO 5. Tallennuskapasiteetti. (Hilbert, 2015)



KUVIO 6. Internetikäyttäjät (*: ennuste). (ITU, 2019)

Tässä vaiheessa voidaan perustellusti kysyä, miten tämä kommunikaation ja tietoliikennetekniikan vallankumous liittyy hybridiuhkiin ja tähän tutkielmaan? Liittyy siten, että nyt käsillä oleva tiedon virran vallankumous moninkertaistaa ihmiskunnan kapasiteetin tiedon taltioimiseen (ks. kuvio 5), levittää ihmisten keskinäisen kommunikaatioverkon globaaliksi (ks. kuvio 6), sekä tekee informaation ja tiedon välittämisen äärimmäisen lyhytviiveiseksi. Ihminen ottaa vastaan ja altistuu tiedolle, informaatiolle, ja pirstaleiselle datalle entistä suuremmissa määrin ja taukoamattomana virtana. Altistumisen käsite ja mielikuva on tässä kohtaa avainasemassa; vaikkemme tietoisesti hakisi jatkuvalla syötöllä uutisia itsellemme tärkeistä asioista tai muista mielenkiinnon kohteistamme, ympäristömme muuttuessa yhä digitaalisemmaksi muun muassa esineiden internetin kautta, mielemme ja tajuntamme, kognitiomme, on arkielämässä jatkuvan tietovirran kohteena.

Informaatio ja kognitio ovat osana myös kybertoimintaympäristön yleisesti hyväksyttyä määritelmää, jossa kybertoimintaympäristö jaetaan kolmeen osa-alueeseen fyysisestä kerroksesta (laitteisto) loogiseen kerrokseen (ohjelmistot), ja kolmanneksi kognitiivinen kerros (informaatio ja ajatukset). (Libicki, 2007, s. 8-9; Nykter, 2018, s. 11) Tämän määritelmän mukaisen kybertoimintaympäristön pohjalta on tehty kyselytutkimus sellaisille suomalaisille organisaatioille, jotka toimivat kansallisen kyberturvallisuuden parissa. Kyselyn perusteella kyberturvallisuudessa korostetaan fyysistä ja loogista kerrosta, kognitiivisen kerroksen jäädessä vähemmälle huomiolle. Tutkimuksessa esitetäänkin johtopäätös, että kognitiivinen osa-alue, käsittäen muun muassa informaatiovaikuttamisen ja informaation manipuloinnin, näyttäytyy kyberturvallisuuden toimijoiden piirissä vähiten ymmäretyiltä ja huomioonotetulta. Syyksi esitetään sitä, että koko osa-alue on vasta viime

vuosina noussut varsinaisesti toimialan yleiseen keskusteluun ja siten kybertoimijoiden tietoisuuteen. (Nykter, 2018, s. 45)

Nämä havainnot vain alleviivaavat entisestään informaatioulottuvuuden tutkimisen tärkeyttä, koska näyttää siltä, ettei informaatiovaikuttamista voi lokeroida osaksi vain jotain tiettyä kattokäsitettä, kuten *kyberturvallisuus* tai *hybridivaikuttaminen*. Pikemminkin vaikka informaatiovaikuttaminen voidaan sijoittaa hybridiuhkien yhdeksi uhkatekijäksi, sen suhteen pitää ymmärtää, että se on toimintatapa, jolla voi vaikuttaa laajasti yhteiskunnan eri osa-alueisiin ja joka voi esiintyä osana melkein mitä tahansa yksittäistä hybridiuhkatekijää. Näin ollen voi loppukaneettina lausua, että on liian yksinkertaistavaa ja vääriä johtopäätöksiä tuottavaa, mikäli informaatiovaikuttaminen käsitellään asiakirjoissa erottamattomasti yhdessä kybervaikuttamisen kanssa, oli kyse vaikkapa sitten tiedustelulakien lakiesityksistä.

4.4 Tulosten vertailu aiempaan tutkimukseen

Vertaillaan seuraavaksi näitä saatuja tuloksia aiemman suomalaisen tutkimuksen tuloksiin, siltä osin kuin tuloksia voidaan vertailla. Tästä aiheesta, kuten tutkielman alkupuolella on mainittu, ei suoranaisesti ole ajantasaista suomalaista tutkimusta tehty, mutta tietyiltä seuraavaksi kerrottavilta osin vertailua on mahdollista tehdä. Kurttila (2015, s. 70) toteaa tutkimuksensa yhteenvedossa, että tiedustelulakien valmistelutekstejä tulkittaessa voidaan nähdä epäilyksiä siitä, että tiedonhankintalaki voi olla ristiriitainen vallitsevan oikeusvaltiokäsityksen kanssa. Tätä samaa ongelmallisuutta on käsitelty myös tässä tutkielmassa, kun mahdollisuus ristiriitaan nähtiin kansainvälisen vertailun luvussa (luku 2.3). Kurttila toteaa myös tutkimustuloksissaan, että tiedustelun lakivalmistelun aikana käydyn keskustelun perusteella itse tiedustelusta ei saa selvää kuvaa eikä myöskään siitä, millaiset tiedonhankintalait itse asiassa tulisi säätää (Kurttila, 2015, s. 71). Tämä voi korreloida tämän tutkimuksen havainnon, tai oikeastaan taustaoletuksen kanssa siinä kohdassa, kun lausutaan että kansallisen uhkaken-tän hybridiuhkat ovat varsin muuttuvia luonteeltaan. Eli voi olla hankala hahmottaa, millaisista uhkista tietoa tulisi hankkia, jos iso osa uhkakuvista muuttuu alati.

Aiemman tutkimuksen vertailussa jatketaan edelleen samassa aiheessa, eli mitä tiedustelusta on puhuttu lakivalmistelun aikaan. Myös Mannonen (2020) on huomannut tutkimuksessaan, että käydyssä eduskuntakeskustelussa korostui kerronta siitä, kuinka maailma muuttuu, ja tämän muutoksen takia viranomaiset tarvitsevat uusia keinoja uhkien torjumiseen (Mannonen, 2020, s. 67). Hän esittää, että turvallistamisteorian näkökulmasta voidaan perustellusti kysyä, että kun hyväksyttiin nykymuotoiset tiedustelulait, hyväksyttiinkö samalla muuttunut turvallisuusympäristö ja uudenlaiset uhkat. Myös tässä tutkielmassa pohditaan turvallisuuskäsityksen ja kansallisten uhkien tiivistä keskinäistä suhdetta (ks. luku 2.4).

Ei kahta ilman kolmatta, eli myös Helenius (2020) on tutkinut tiedustelulakeja juuri niistä käydyn eduskuntakeskustelun, mukaan lukien valiokunnat, perusteella. Hän tutkimustuloksissaan päätyy samansuuntaisiin havaintoihin ja tuloksiin kuin kaksi edellä esiteltyä tutkimusta: tiedustelutoiminnan oikeusvaltiolliset laillisuusnäkökulmat olivat keskeisesti esillä läpi tarkastelun kohteena olleissa keskusteluissa (Helenius, 2020, s. 108). Hän huomauttaa, että tutkimuksen kohteena on siviilitiedustelulaki ja Suojelupoliisi, eikä tutkimuksessa tehty vertailua sotilastiedustelulakiin, vaikka se olisi hänen mukaansa olisi voinut olla mielenkiintoista esimerkiksi siinä mielessä, että olisiko sotilastiedustelulain perusteluissa korostettu eri uhkatekijöitä kuin siviilitiedustelulakiesityksessä (Helenius, 2020, s. 109).

Täytyy mainita, että tässä käsillä olevassa hybridiuhkia ja tiedustelulakeja vertaavassa tutkimuksessa huomattiin hallituksen tiedustelulakiesityksistä (HE 202/2017 ja 203/2017) se, että hallituksen esityksessä sotilastiedustelulaeista oli ajoittain hieman seikkaperäisempiä perusteluja kuin siviilitiedustelun lakiesityksessä. Esimerkiksi sotilastiedustelulain perusteluissa käsitellään useassa kohtaa disinformaatiota, mutta siviilitiedustelulakiesityksessä ei juuri ollenkaan. Muutoin keskeinen huomio on se, että lakiesitykset sisälsivät varsin paljon samaa tekstiä, kuten kuvaukset Suomen toiminta- ja turvallisuusympäristöstä.

Ja viimeisenä tästä aiheesta, myös Tanner (2019) tutki tiedustelulakeja keskustelujen kautta, sillä hänellä tutkimusaineistona on poliittiset keskustelut tiedustelulainsäädännöstä. Tutkimuksessa pyrittiin keskusteluja analysoimalla hakemaan vastausta siihen, että onko Suomessa todellinen turvallisuusongelma, eli onko meillä kansallisella tasolla uhkia, joihin ei kyetä vastaamaan. Vai onko tiedustelulakien luomisessa kyse pikemminkin turvallistamisongelmasta. Turvallistamisella Tanner (2019, s. 24) tarkoittaa sitä (viitaten aiempiin tutkimuksiin turvallistamiskäsitteestä), että kun annetaan väite jonkin asian olevan turvallisuuskysymys, on se väite samalla kannanotto siitä, että tämä asia uhkaa turvallisuuttamme. Eli esitettävä asia turvallistetaan. Tanner (2019, s. 54) toteaa, että tiedustelulakien valmistelussa esiintyi useita turvallistamisen prosesseja (Tanner, 2019, s. 54). Yksi keskeinen turvallistamisen prosessi oli hänen mukaansa kybertoimintaympäristön turvallistaminen, joka alkoi vuonna 2013 lanseeratun kyberturvallisuusstrategian myötä. Mutta hän myös huomaa tutkimuksessaan sen, että kyberturvallisuuden tutkiminen ja keskustelu siitä on vielä lapsenkengissä, joka oletettavasti johtuu siis koko kyseisen turvallisuuden osa-alueen erittäin nuoresta iästä (Tanner, 2019, s. 54–59). Myös tässä tutkimuksessa kiinnitettiin huomiota kyberturvallisuuden nuoruuteen, tai oikeastaan paremminkin digitaalisen viestinnän nuoruuteen, kun luvussa 2.4 mainitaan, että nykymuotoinen globaali digitaalinen kommunikaatio on syntynyt vasta aivan viime vuosikymmeninä. Ja edelleen luvussa 4.3 esitetään kuvioin, kuinka varsinaisesti vasta 2010-luvulla on digitaalisen viestinnän piiriin siirtynyt valtaosa osa maapallon väestöstä. Tähän tilastotietoon peilaten on selitettävissä, miksi kybertoimintaympäristöön ja tietoliikenteeseen liittyvät uhkakuvat ovat varsin nuoria – digitaalinen viestintä ei ole ollut globaalia valtavirtaa vielä muutamia vuosikymmeniä sitten.

Kun on juuri sanottu, että tutkimuksissa koskien tiedustelulaeista käytyä keskustelua korostuu laillisuusnäkökulmat, on tutkimusta tiedustelulaeista tehty myös spesifisti tiedustelun valvonnan toteuttamisen näkökulmasta (Pekola, 2018). Myös hänen tutkimuksensa yksi keskeinen havainto on se, että tiedustelutoimivaltuuksien saannin välttämättömyyttä perustellaan muuttuneilla uhkakuvilla (Pekola, 2018, s. 105). Kyseisen tutkimuksen johtopäätöksissä korostuu myös se, että Suomen kaltaisessa oikeusvaltiossa tulee tiedustelutoimivaltuuksien yhteydessä ottaa myös huomioon perus- ja ihmisoikeusvelvoitteet (Pekola, 2018, s. 108). Tämän tutkimuksen havainnot tukevat edelleen kaikkea edellä esitettyä, kuin myös tämän tutkimuksen havaintoja.

Viimeisenä aiemman tutkimuksen verrokkiaineistona toimii teos, jossa tutkitaan itse tiedustelutoimintaa. Siljoranta (2020) tutkii tiedustelulakeja ja avointen lähteiden tiedustelua. Tässä tutkimuksessa ei ole kovinkaan paljoa vertailukohtaa tämän tutkimuksen tuloksiin, sillä Siljoranta toteaa, että tiedustelulakeja tutkimalla selviää, ettei avointen lähteiden tiedustelu vaadi erillistä toimivaltuutta (Siljoranta, 2020, s. 67). Ja koska tässä tutkimuksessa peilattiin hybridiuhkia nimenomaan annettuihin tiedustelutoimivaltuuksiin, luisui avointen lähteiden tiedustelu automaattisesti ulos tutkimuksellisen fokuksen alta. Kuitenkin kaikkien muiden tapaan, myös Siljoranta (2020, s. 68) toteaa, että keskeisenä taustatekijänä vaikuttamassa suomalaisten tiedustelulakien syntyyn oli muuttunut turvallisuusympäristömme.

Yhteenvedona kaikista näistä vertailluista aiemmista tutkimuksista voidaan lausua ainakin se, että yhteisesti tämän hetken tutkimuksissa todetaan se, että turvallisuuden ja uhkakuvien luonnetta pidetään muuttuvana. Ison painoarvon tiedustelulakeihin liittyvässä diskurssissa saa myös ihmisoikeuksien toteutumisen ja tiedonhankinnan tarpeen keskinäissuhteeseen liittyvä tasapainoilu.

5 TUTKIMUKSEN JOHTOPÄÄTÖKSET

Tutkimuksen aikana koodattiin valitun tutkimusmetodin mukaisella tavalla sivumääräisesti runsas määrä eri viranomaisten, ministeriöiden sekä hallituksen dokumentteja. Monia mielenkiintoisia seikkoja nousi useassa kohtaa esille, ja tästä johtuen tutkimuksen yhteenvedossa ja johtopäätöksissä on pyritty erityiseen huolellisuuteen niin luvun pituuden kuin laadun suhteen; kaikkia esiin nousseita seikkoja tai mielenkiintoisia tekstikohtia ei ole järkevää eikä tarkoituksenmukaista nostaa esiin. Tällöin tutkielman ydinsisältö hukkuisi isoon, vaikkakin tästä aihealueesta kiinnostuneelle lukijalle toivottavasti mielenkiintoiseen, massaan.

Tässä pääluvussa esitetään tiivis pohdinta tutkimuksen luotettavuudesta ja toistettavuudesta, jota seuraa havaittujen jatkotutkimustarpeiden esittely. Pääluku ja koko tutkielma päätetään pohdintaan tutkielman aiheesta sekä tutkimuksen teon aikana heränneistä sellaisista seikoista, jotka eivät muussa kohti tutkielmaa ole tulleet esille.

5.1 Tutkimuksen luotettavuudesta ja toistettavuudesta

Valittu tutkimusmetodi, ankkuroitu menetelmä, tuo siinä mielessä tutkimukseen jo itsessään luotettavuutta, koska tutkimusaineisto on pitänyt tarkastella järjestelmällisesti sivu sivulta. Lisäksi tutkijan tekemät virheet, laiminlyönnit tai taustaoletukset ovat pakotetusti minimoidut, koska aineistoa tutkittiin sillä johtajatuksella, että kaikki teksteissä olevat hybridivaikuttamiseen tai -uhkiin liittyvät asiat tulee huomioida ja nostaa tutkielmaan sellaisenaan. Tästä osoituksena on runsas määrä tutkielman liitteitä, joissa on käsiteltoilla kerrottu, mitä kukin tutkimusaineistodokumentti piti sisällään hybridivaikuttamiseen liittyen. Tämä ei kuitenkaan poista tarvetta arvioida tutkimuksen luotettavuutta, sillä kaikessa tieteellisessä tutkimuksessa tulee suorittaa tehdyn tutkimuksen luotettavuusarviointia (Hirsjärvi ym., 2016, s. 231).

Tutkimuksen luotettavuuden määrittämiseen on eri mittareita. Keskeinen mittauksen kohde on tutkimuksen validiteetti. Validiteetti tarkoittaa muun muassa sitä, kuinka soveltuva tutkimukseen valittu tutkimusmenetelmä on, kun sitä käyttämällä ratkaistaan asetettua tutkimusongelmaa (Hirsjärvi ym., 2016, s. 231). Validiteetti jakautuu eri alakäsitteisiin, joita ovat muun muassa käsitevaliditeetti, korrelatiivinen validiteetti, sekä kontekstivaliditeetti (Hiltunen, 2009, s. 6-7). Käsitevaliditeetin avulla pohditaan sitä, onko tutkimuksen teoreettinen lähestymistapa valittu oikein ja onko tutkittavan ilmiön luonnetta tulkittu oikein. Käsitevaliditeetin tärkeys korostuu, jos tutkimukseen on asetettu tutkimushypoteeseja. Korrelatiivinen validiteetti taas tarkoittaa sitä, kuinka tutkimuksen tuloksilla on korrelaatiota toiseen saman aihealueen tutkimuksessa saatuihin tuloksiin. Ja kolmantena kontekstivaliditeetti, jonka avulla arvioidaan sitä, kuinka hyvin tutkimusaineisto liittyy tutkittavaan ilmiöön ja onko jokaisella tutkimusaineiston osalla jokin yhteys saatuun tutkimustulokseen. (Hiltunen, 2009, s. 6-7)

Seuraavaksi peilataan tutkimusta näihin esiteltyihin validiteetin eri alakäsitteisiin. Mitä käsitevaliditeettiin tulee, niin tutkimuksessa ei ole erityistä tutkimushypoteesia, jota testattaisiin valitun tutkimusaineiston kautta. Kuitenkin tutkimuksessa tehdään tietynlainen oletus hybridivaikuttamisen muuttuvasta luonteesta, joka ilmenee jo tutkielman otsikossa. Mutta myös se on kirjoitettu esiin, että laajemmaltikin pidetään todellisena tätä hybridivaikuttamisen muuttuvaa ja yllätyksellistä luonnetta. Esimerkiksi tämä tutkielma alkaa puolustusministeriön kansliapäällikön (Juusti, 2021) lainauksella juurikin hybridivaikuttamisen yllättävästä luonteesta. Myös muissakin kohdin tämä muuttuva luonne tulee ilmi, vaikkapa kun Suojelupoliisi tunnistaa hybridiuhkien kenttään 'muut toimet' -kategorian, jolla tarkoitetaan niitä hybridivaikuttamisen keinoja, joita emme tällä hetkellä osaa tunnistaa tai kuvitella. Voitaneen siis todeta, että hybridivaikuttamisen ilmiötä tulkitaan oikein, kun sen todetaan olevan muuttuva luonteeltaan.

Korrelatiivinen validiteetti on siinä mielessä haastava, että spesifisti tästä aiheesta ei ole muuta suomalaista tutkimusta. Vertailu jonkin toisen valtion tiedustelulainsäädännöstä tehtyyn tutkimukseen ei todennäköisesti olisi hedelmällistä. Tämän voi sanoa sillä perusteella, kun luvussa 2.3, jossa esiteltiin eräiden muiden valtioiden tiedustelutoimivaltuuksia, huomattiin että eri valtioiden kansalliset tiedustelulainsäädännöt eroavat keskenään. Tämä kansainvälinen vertailu osoittaa kuitenkin sen, että ainakin osassa muissakin länsimaissa tiedustelutoiminnalla pyritään hankkimaan tietoa laajasti yhteiskunnan vakautta horjuttavista uhkista, eikä tiedonhankintaa ole rajoitettu kohdistumaan vain tietyn tyyppisiin uhkiin, kuten terrorismiin tai sotilaallisiin uhkiin. Tämä havainto korreloi tämän tutkimuksen lopputuloksen kanssa, eli suomalainen tiedustelulainsäädäntö mahdollistaa laajan tiedonhankinnan niistä uhkista, mitä suomessa käsitetään hybridiuhkien kenttään kuuluviksi. Myös Suojelupoliisi itse on lausunut, että he ovat virastona tyytyväisiä nykymuotoisiin tiedustelulakeihin (Pelttari, 2021). Tämä lausunto korreloi

tämän tutkimusten tulosten kanssa, eli tiedustelulakien mandaateilla voidaan hankkia tietoa nykymuotoisista hybridi vaikuttamisen keinoista.

Viimeisen validiteettikäsitteen, kontekstivaliditeetin, asettamat vaatimukset pyritään täyttämään tämän tutkielman tutkimusaineiston osalta siten, että hybridiuhkakäsitteen muodostamiseen ei ole käytetty pelkästään niitä lähteitä, mitkä tutkijan mielestä on relevantteja. Päinvastoin, hybridiuhkakäsitteen tutkimusaineisto valikoitui suomalaisen uhkakuvia käsittelevän tietoteoksen (Linnell & Iloniemi, 2018) perusteella, eikä tutkijan näkemysten perusteella. Jokaiselle tutkimusaineiston osalle ja teokselle annettiin yhtäläinen painoarvo, ja jokainen teos antoi yhtä suuren osan lopullisen hybridiuhkakäsitteen muodostukseen. Tämä prosessi on läpinäkyvä, sillä jokaisen yksittäisen tutkimusaineistodokumentin käsittely on avattu tutkielman liitteissä oleviin käsittekarttoihin.

Luotettavuuden lisäksi tutkimuksen laatua mitataan tutkimuksen toistettavuudella, josta käytetään myös sanaa reliabelius (Hirsjärvi ym., 2016, s. 231). Sillä tarkoitetaan muun muassa sitä, että tutkimuksessa osoitetaan se tapa, millä lopputulokseen on päästy, sekä kerrotaan ne muuttujat, jotka ovat olleet vaikuttamassa syntyneeseen lopputulokseen. Määrällisessä tutkimuksessa tämä on helppo käsitellä numeraalisina arvoina, mutta laadullisessa tutkimuksessa on erityisen tärkeää osoittaa se, millä tavoin laadullista aineistoa on tutkittu. Ja koska ankkuroidun menetelmän tutkimuksessa korostuu aineiston erittäin yksityiskohtainen tarkastelu, on tutkimustapaa avattu luvussa 3.3. Tutkimuksen aikana painotettiin myös sitä, ettei tutkijan ennako-oletuksille annettu mitään sijaa, vaan kaikki tutkimustuloksiin vaikuttavat seikat nousivat kirjallisesta aineistosta, vaikka tämä olisi tarkoittanut ennako-oletusten vastaisia tuloksia. Erityisen tyydyttävää tieteellisen tutkimuksen teko itse asiassa tällöin onkin, kun muodostettava tieto muuttuu ja rikkoo vanhoja käsityksiä.

5.2 Jatkotutkimustarpeet ja -mahdollisuudet

Kun läpi tutkielman on puhuttu hybridiuhkien ja uhkakuvien muuttuvasta luonteesta, jonkinlainen seurantatutkimus siitä, kuinka uhkakuvat ovat valtiollisessa narratiivissa todella muuttuvat, olisi mielenkiintoista. Myös määrällistä tutkimusta sen suhteen voisi tehdä, kuinka eri vuosina julkaistuissa asiakirjoissa mikäkin uhkatyyppi saa painoarvoa, esimerkiksi sanamääräisen esiintyvyyden suhteen. Toinen vaihtoehto tutkia uhkakuvien muuttuvaa luonnetta, olisi keskittyä tutkimaan uhkakuvien ennustettavuutta. Nykypäivänä voisi tutkia lähitulevaisuuteen peilaavia tavoiteohjelmia tai ennusteita, kuten Sisäministeriön laatiman 'Sisäisen turvallisuuden tulevaisuuskuva 2025' kirjauksia tai Eduskunnan Tulevaisuusvaliokunnan julkaisuja. Ja sitten ajan kuluessa voisi peilata näitä asiakirjoja oikeasti tapahtuneeseen kehitykseen. Näin olisi mahdollista arvioida, kuinka hyvin

osaamme ennakoida turvallisuus- ja uhkakehityksiä. Tällainen tutkimus edellyttää toki mahdollisuutta ja resursseja pitkäjänteiseen tutkimustyöhön.

Tiedustelulakien osalta olisi mielenkiintoista tehdä tutkimusta siinä vaiheessa, kun sellaisia julkaisuja ilmestyy, jotka käsittelevät tiedustelulakien toimivuutta. Tällä hetkellä, vuonna 2022, tunnustetaan ainakin osassa kansanedustajien puheenvuoroissa tiedustelulakiaiheeseen liittyen, että juuri kattavampaa kuvaa tarvitaan tiedustelulakien toimivuudesta ennen kuin pohditaan sitä, kuinka tiedonhankintatoimivaltuuksia tulee päivittää (Joentausta, 2022; Pietiläinen, 2022). Toimivuutta analysoivien julkaisujen tieteellinen tarkastelu ja vertailu tiedustelulainsäädännön lakiesityksiin ja lähetekeskusteluihin voisi paljastaa, mitä tiedonhankintatarpeita – eli siis kansallisia uhkia – emme osanneet nähdä 2010-luvulla.

Koska informaatiovaikuttaminen näyttäytyi tutkimuksessa niinkin mielenkiintoisena hybridivaikuttamisen keinona, että siitä kirjoitettiin myös omassa alaluvussa (luku 4.3, joka ei tosin ole pyhitetty pelkästään informaatiovaikuttamiselle), on syytä mainita yksi näkökulma myös siitä. Keskeinen kysymys tällä hetkellä on, globaalistikin, että pitäisikö informaatiovaikuttamiseen kyetä vastaamaan valtiollisella tasolla ja valtiovallan toimenpitein? Yhdysvalloissa on esimerkiksi pohdittu niin sanotun algoritmiviraston perustamista (Helin & Rigatelli, 2021), jota aihetta sivutaan vielä seuraavassa pohdintaluvussakin. Tämän vaikuttamiskanavan vakavuutta ja merkittävyyttä olisi mielenkiintoista tutkia, sillä aivan viimeaikaiset alustavat tutkimukset Suomessakin osoittavat, että sosiaalisen median vaikuttavuus ihmisten äänestyskäyttäytymiseen on merkittävä (Niemonen, 2021), ja lisäksi Yhdysvalloissa arvioidaan että Trumpin kauden jälkeiset levottomuudet eivät tule olemaan viimeisiään laatuaan (Tikka, 2021). Myös aivan tuoreena informaatiovaikuttamisen esimerkkinä nähdään Venäjän pyrkimyksiä ohjata keskustelua ja hakea pieniäkin vivahde-eroja länsimaisten valtioiden narratiiveista liittyen meneillään olevaan Ukrainan konfliktiin (Luotonen, 2022). Kovasti informaatiovaikuttaminen nähdään siis ainakin huolestuttavana ilmiönä, mutta sitä, kategorisoidaanko se kansallista turvallisuutta uhkaavaksi vaikuttamiskeinoksi, voi olla haastavampi lausua, ainakaan ilman tutkimusta aiheesta. Myös tutkimusta siitä, kuinka informaatiovaikuttamiseen voi tehokkaimmin vastata, voisi olla perusteltua tehdä. On esitetty lausuntoja, että medialukutaidon vahvistaminen olisi avain disinformaation kitkemiseksi (Sandell, 2021), ja tätä voisikin olla mielekästä tutkia – mikä on tehokkain keino madaltaa informaatiovaikuttamisen tehoa? Voisiko määrällisen tutkimuksen keinoin selvittää ihmisen koulutustason kausaliteettia kykyyn kriittiseen ajatteluun ja disinformaation huomaamiseen. Vai tulisiko pikemmin tehdä tutkimusta monimuuttuja-analyysin keinoin, jossa ylipäätään etsitään vahvinta kausaliteettia, kun perusmuuttujana tämän syy-seuraussuhteen toisella puolella on kyky huomata ja sietää (eli ettei disinformaatio vaikuta omaan toimintaan) disinformaatiota.

5.3 Pohdinta

Tiedustelulakeja tutkiessa tuli monessa kohtaa ilmi, tiedustelutoimialaan vihkiytyneille ehkä itsestäänselvyys, että tiedustelulla ei lähtökohtaisesti varsinaisesti torjuta uhkia, vaan muu lainsäädäntö ja viranomaistoimivalta on välttämätöntä torjuntatoimien toteuttamiseksi. On varmasti tilanteita, joissa uhkatoimijan kokemus paljastumisen riskistä tai tiedustelun kohdistumisesta häneen riittää lopettamaan uhkatoiminnan, mutta viimeaikaiset esimerkit ovat osoittaneet, että hybridiuhkien torjuntaan tarvitaan laaja-alaista lainsäädännön kehittämistä. Krimin miehitys tunnuksittomilla, mutta selvästi järjestäytyneillä ja aseellisesti varustautuneilla joukoilla aiheutti tarpeen aluevalvontalain muutokselle, koska vuosituhannen alussa säädetty aluevalvontalaki tunnisti tuolloin vihamieliseksi henkilön tai henkilöjoukon toiminnaksi vain vieraan valtion asevoimiin kuuluvan, sotilaallisin tunnuksin varustetun henkilön tai joukon toteuttaman toiminnan (HE 56/2017, s. 16). Lakimuutostarvetta perusteltiin nimen omaan tarpeella kasvattaa kykyä hybridiuhkien torjuntaan (HE 56/2017, s. 3–4). Tämän tutkielman hybridiuhkakäsitteen sisällä tämänkaltaista toiminta profiloituisi ensisijaisesti epävarman ja ennustamattoman turvallisuusympäristön luonnin sisälle (sekä informaatiovaikuttamista, mikäli toimintaan liittyy osallisuuden kiistäminen), ja mikäli toiminta on avoimen väkivaltaista, liukuu toiminta perinteiseen uhkakuvakenttään sotilaallisen voimankäytön uhkaan.

Tuoreempi esimerkki on syntynyt loppukesän ja syksyn 2021 tapahtumista Valko-Venäjän, Puolan ja Baltian maiden rajatapahtumista, jossa on osoitettavissa valtiojohtoista pakolaistoiminnan ja maahantulon järjestämistä (Hiltunen, 2021). Tämän tiimoilta on syntynyt Suomessa poliittista debattia siitä, tulisiko rajavartio- ja ulkomaalaislakia päivittää, jotta viranomaisilla on käytössä tarvittava toimivaltuus keskeyttää tai estää turvapaikanhaku, mikäli on osoitettavissa, että maahantulijoita käytetään hybridivaikuttamisen keinona (Toivonen, 2021). Tällainen toiminta asettuisi tämän tutkielman hybridiuhkakäsitteen kentässä painostamisen uhkatekijän sisälle.

Viimeisenä esimerkkinä voi mainita asiantuntijoiden keskusteluun nostamat tarpeet valmiuslain muutoksille, perustuen tarpeeseen kyberuhkien torjuntaan (Linnéll & Kari, 2020). Samassa yhteydessä nostetaan esiin tarve myös aluevalvontalain päivitykselle, juuri kybertoimintaympäristön uhkien torjuntaan ja vastaamiseen. Juuri aluevalvontalain päivitystarpeen esilletuonti on mielenkiintoinen yksityiskohta, sillä kuten edellisessä esimerkissä kerrottiin, kyseistä lakia päivitettiin vain muutama vuosi ennen tätä asiantuntijakirjoitusta. Kertooko tämä hybridiuhkien nopeasyklisestä ja vaikeasti ennustettavissa olevista kehityskuluista?

Juuri tähän kysymykseen tulisi tiedustelulla voida vastata, jotta toimivaltuusasiat uhkien torjuntaan eivät olisi reagoivassa tilassa, vaan pikemminkin ennakoivassa tilassa. Tällä tarkoitetaan sitä, että hybridiuhkien torjunnassa ollaan auttamattomasti jäljessä, jos vasta havaittu toiminta

aiheuttaa kansallisen keskustelun siitä, tulisiko nyt jo tapahtuneeseen toimintaan kyetä vastaamaan tulevaisuudessa. Tiedustelun lakisääteinen tehtävä on hankkia myös strategisen, eli pitkälle tulevaisuuteen katsovan, suunnittelun tueksi ilmiötason uhkatietoa (Hakonen, 2020a, s. 7). Tämä tehtävä on toki helposti sanottu ja annettu, mutta todennäköisesti vaikeasti toteutettava – kuinka arvioida tulevaisuutta hybridiuhkien osalta, kun koko käsite on maturiteetiltaan varsin nuori ja tietyiltä osin jopa kiistanalainen (kuten hybridi-etuliitteen käyttäminen eri uhkakuvissa, mm. sodankäynnissä; ks. Hyytiäinen, 2017, s. 17)? Voisiko yksi hiljainen signaali tulla Yhdysvalloista, jossa on Trumpin presidenttikauden loppupuolella ja jälkeen käyty kipeääkin itsereflektiota sosiaalisen median voimasta, ja osana sitä on pohdittu tarvetta niin sanotun algoritmiviraston perustamiselle, jonka tarkoituksena olisi säännellä ja valvoa niitä teknisiä mekanismeja, jotka valitsevat, minkälaisen sisällön näkyvyyttä edistetään sosiaalisessa mediassa (Helin & Rigatelli, 2021). Myös Euroopassa on tutkittu vastaavaa teemaa, eli valtiojohtoisen tai jopa ylikansallisen sääntelyn tarvetta algoritmeille, mitkä tekevät päätöksiä ihmisten tiedostamatta, kuten valintoja siitä, mitä sisältöä näytetään ensisijaisesti sosiaalisen median uutisvirroissa (Bejtullahu-Michalopoulos & Florin, 2018). Ehkä yhtenä seurattavana mittarina hybridiuhkien kehittymisen tutkimisessa voisi toimia tieteellisen keskustelun määrä ja painopiste; mitä enemmän jonkin tietyn turvallisuushuolia herättävän aiheen tutkimiseen osoitetaan resursseja, sitä relevantimpi ja todennäköisempi tulevaisuuden uhkakuva se todellakin on. Ja jos esitetään kritiikkiä sillä perusteella, että kuinka todennäköistä on se, että kaikkia mahdollisia keinoja jokin taho käyttäisi valtiolliseen vaikuttamiseen, niin vasta-argumenttina voidaan viitata vaikkapa kiinalaisia teoksia rajoittamattoman sodankäynnin opista. Tässä opissa pääpaino on sellaisissa aggressiivisissa toimissa, joita voidaan tehdä ilman sodanjulistusta, sekä ottaa valtiollisen vaikuttamisen keinovalikoimaan kaikki mahdolliset toimet, joilla vastapuoleen voidaan vaikuttaa (Chew, 2018; Liang & Xiangsui, 1999).

Kansallisen tiedustelutoimintamme tarkoitus on parantaa suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuutemme kohdistuvilta kaikkein vakavimmilta uhkilta (HE 202/2017, s. 1). Tiedustelulainsäädäntöhankkeen tarve nähtiin syntyneen erityisesti monimutkaistuneen turvallisuusympäristön ja hybridivaikuttamisen sekä -uhkien synnyn myötä, sekä lisäksi tarpeesta luoda säädöspohja tiedustelutoiminnalle (HE 203/2017, s. 126; HE 202/2017, s. 108). On siis erityisen tärkeää, että tiedustelulait muotoillaan huolellisesti kestäväksi aikaa, kun maailma ja toimintaympäristö muuttuu vauhdilla. Edelliset esimerkit viime vuosien lakiuudistuksista ja uudistustarpeista kertoo hybridiuhkien muuttuvasta luonteesta. Tutkielmassa ilahduttavasti huomattiin, että tiedustelulait antavat tiedonhankinnan mandaatin varsin kattavasti nykykäsitteiden mukaisesti hybridiuhkiin, eikä lopullisessa lakitekstissä ole sorruttu liian spesifiin raamittamiseen.

Tiedustelutiedon hankkimisen ja siitä valmiin tiedustelutuotteen luomisen jälkeen on vaihe, jossa tieto esitellään ja luovutetaan päätöksentekijälle ja myös

lopulta se, kuinka tiedustelutietoa käytetään päätöksenteon tueksi. Tämä tutkielma keskittyi tiedustelutoiminnan, niin sanotun tiedustelusyklin, alkuvaiheisiin, jos tavoitevaiheena pidetään tiedon tai tuotteen luovuttamista tiedon tarvitsijalle. Paraskaan tiedustelulaki tai toimivaltuus ei auta, mikäli realisoituu se riski, että vaikka relevantti tieto saadaan kerättyä tiedustelun menetelmin, mutta se ei ikinä päädy oikea-aikaisesti päätöksentekijän käyttöön. Tai vaikka päätyisikin käytettäväksi, niin saatuun tietoon ei luoteta tai sitä ei haluta uskoa. Bellingcat-ryhmän perustaja Eliot Higgins kuvaa tätä dilemmaa ryhmästä kertovasta kirjassa, kun hän jakaa kokemuksiaan siitä, kuinka hänen löydöksiään vastustettiin ja niitä, sekä häntä ihmisenä, pyrittiin mustamaalaamaan (Higgins, 2021, s. 57). Näin ollen, tutkielman viimeisenä johtopäätöksenä ja pohdintana sanottakoon se, että samalla kun suomalainen tiedustelutoiminta kehittyy ja vakiinnuttaa asemansa, on ensiarvoisen tärkeää käydä avointa yhteiskunnallista keskustelua tiedustelutoiminnasta. Tähän keskusteluun tulee sisällyttää aiheita niin oikeusvaltioperiaatteiden toteutumisen näkökulmasta kuin tiedustelulakien tehokkuudesta, kun turvallisuusviranomaiset pyrkivät ennakoivasti hankkimaan tietoa uhkista, jotka ovat luonteeltaan muuttuvia. Näin on edellytys ylläpitää sitä yhteiskunnallista olotilaa, jossa kaikilla yhteiskuntamme jäsenillä säilyy luottamus ja tuki suomalaiseen tiedustelutoimintaan.

LÄHTEET

- Aaltomaa, K. (2017). Osastopäällikkö, Sisäministeriön poliisiosasto. *Siviilitiedustelulainsäädäntö suojaisi kansallista turvallisuutta* (siviilitiedustelulainsäädännön työryhmän puheenjohtajan puheenvuoro). Tiedustelumietintöjen luovutus 19.4.2017, kohdasta 01:30 - 11:20. Haettu 22.1.2021 osoitteesta <https://sisaministerio.videosync.fi/tiedustelu>
- Abbott, D. (toim.). (2010). *The Handbook of 5GW: A Fifth Generation of War?* Ann Arbor: Nimble Books.
- Allcott, H. & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspective* 31(2), 211–236. Haettu 8.11.2021 osoitteesta <http://dx.doi.org/10.1257/jep.31.2.211>
- Bartuška, V., Lang, P. & Nosko, A. (2019). The Geopolitics of Energy Security in Europe. Teoksessa T. Valášek (toim.), *New Perspectives on Shared Security: NATO's Next 70 Years*. Brussels: Carnegie Europe. Haettu 2.11.2021 osoitteesta https://carnegieendowment.org/files/NATO_int_final1.pdf
- Bejtullahu-Michalopoulos, K. & Florin, M-V. (2018). *Workshop Report: The Governance of Decision-Making Algorithms*. Lausanne: EPFL International Risk Governance Center. Haettu 16.11.2021 osoitteesta <https://doi.org/10.5075/epfl-irgc-261264>
- Blombergs, F. (2013). *Euroopan voimatasapainojärjestelmä 1990-2012 : Euroopan vakaas rakenteellisen, uusklassisen ja hegemonisen realismin näkökulmasta*. Maanpuolustuskorkeakoulu, Strategian laitos. Julkaisusarja 1: Strategian tutkimuksia No 32. Haettu 3.6.2021 osoitteesta <http://urn.fi/URN:ISBN:978-951-25-2440-2>
- Brun, M. & Pedersen, T. (2019). *Denmark is losing jobs with new cybersecurity law*. Blogikirjoitus 5.2.2019. Haettu 17.6.2021 osoitteesta <https://www.linkedin.com/pulse/denmark-losing-jobs-new-cybersecurity-law-mikkel-hippe-brun>
- Cerulus, L. (2019). *How Ukraine became a test bed for cyberweaponry*. Artikkelijulkaisussa Politico. Haettu 9.11.2021 osoitteesta <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>
- Charmaz, K. (2014). *Constructing Grounded Theory*. 2. painos. London: SAGE Publications Ltd.

- Chew, J. (2018). *How China Applies its "Principles of Unrestricted Warfare" in the 21st Century*. Raportti, Galisteo Consulting Group. Haettu 30.11.2021 osoitteesta <https://www.researchgate.net/publication/325455484>
- Cole, D. & Dempsey, J. (2006). *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: New Press.
- Corbin, J. & Strauss, A. (2015). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 4. painos. Thousand Oaks, CA: SAGE Publications Inc.
- Council of Europe. (2016). *Mass surveillance - Who is watching the watchers?* Strasbourg: Council of Europe Publishing.
- CSIS. (2021). *Significant Cyber Incidents*. Haettu 9.11.2021 osoitteesta <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
- Deflem, M. & McDonough, S. (2015). The Fear of Counterterrorism: Surveillance and Civil Liberties Since 9/11. *Society*, 52(1), 70–79. Haettu 21.12.2021 osoitteesta <http://dx.doi.org/10.1007/s12115-014-9855-1>
- Donohue, L. (2016). *The Future of Foreign Intelligence : Privacy and Surveillance in a Digital Age*. Canada: Oxford University Press.
- Eduskunta. (2019). *Tiedustelulait*. (T. Peuhkurinen, toim.) Lakihankkeiden tietopaketti, Eduskunnan kirjasto. Aineisto päivitetty 9.5.2019. Haettu 22.2.2021 osoitteesta <https://urly.fi/1WiB>
- Eerola, A. (2014). *Uusia syytöksiä venäläislasten kaltoinkohtelusta Suomessa*. Iltalehti uutiset, 17.11.2014. Haettu 2.11.2021 osoitteesta <https://www.iltalehti.fi/uutiset/a/2014111718843851>
- Euroopan parlamentti. (2019). *Euroopan parlamentin päätöslauselma 12. maaliskuuta 2019 EU:n ja Venäjän poliittisten suhteiden tilasta*. T8-0157/2019. Haettu 28.10.2021 osoitteesta https://www.europarl.europa.eu/doceo/document/TA-8-2019-0157_FI.html
- Fujiwara, T., Müller, K. & Schwartz, C. (2020). *The Effect of Social Media on Elections: Evidence from the United States*. Haettu 8.11.2021 osoitteesta <https://dx.doi.org/10.2139/ssrn.3719998>
- Georgacopoulos, C. & Mores, G. (2020). *How Fake News Affected the 2016 Presidential Election*. Artikkelijulkaisussa Louisiana State University, LSU.

Haettu 8.11.2021 osoitteesta
<https://faculty.lsu.edu/fakenews/elections/sixteen.php>

Giannopoulos, G., Smith H. & Theocharidou, M. (2021). *The Landscape of Hybrid Threats : A Conceptual Model*. European Commission. Haettu 22.2.2021 osoitteesta <https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/>

Glaser, B. & Strauss, A. (1967). *The Discovery of Grounded Theory : Strategies for Qualitative Research*. Chicago: Aldine Publishing.

Glaser, B. (1992). *Basics of Grounded Theory Analysis : Emergence Vs. Forcing*. Mill Valley: Sociology Press.

Graaff, B. (2014). By way of introduction: a systemic way of looking at the future of intelligence. Teoksessa B. Jong, I. Duyvesteyn & J. Reijn (toim.), *The Future of Intelligence: Challenges in the 21st century*. New York: Routledge.

Hakonen, K. (2020a). *Tiedusteluvalvontavaltuutetun kertomus vuodelta 2019*. Eduskunnan valtiopäiväasia K 14/2020 vp. Haettu 10.5.2021 osoitteesta <https://www.eduskunta.fi/pdf/K+14/2020>

Hakonen, K. (2020b). *Tiedustelutoiminnan organisointitapoja – vertailussa Pohjoismaat*. Kolumni 2.9.2020. Haettu 22.6.2021 osoitteesta <https://tiedusteluvalvonta.fi/-/tiedustelutoiminnan-organisointitapoja-vertailussa-pohjoismaat>

Harari, Y. (2011). *Sapiens. Ihmisen lyhyt historia*. (J. Iso-Markku, suom.) 8. painos. Liettua: ScandBook UAB.

Harding, L. (2017). *Vaiennettu: agentti Litvinenkon murha ja Venäjän sota lännen kanssa*. (U. Lempinen, suom.) Latvia: Dardedze holografia.

HaVM. (30/2018). *Hallituksen esitys eduskunnalle siviilitiedustelua koskevaiksi lainsäädännöksi*. Hallintovaliokunnan mietintö 6.2.2019. Haettu 19.7.2021 osoitteesta https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_30+2018.pdf

Havulinna, M. (2018). *Kansallinen turvallisuus vs. perusoikeudet: Lainsäädäntötutkimus tiedustelulakihankkeesta* (Pro gradu -tutkielma). Turun yliopisto. Haettu 13.7.2021 osoitteesta <http://urn.fi/URN:NBN:fi-fe2018100837838>

- HE. (264/2006). *Hallituksen esitys Eduskunnalle puolustusvoimалаiksi ja eräksi siihen liittyviksi laeiksi.* Haettu 19.7.2021 osoitteesta <https://www.finlex.fi/fi/esitykset/he/2006/20060264.pdf>
- HE. (346/2014). *Hallituksen esitys eduskunnalle laiksi poliisin hallinnosta annetun lain muuttamisesta ja eräksi siihen liittyviksi laeiksi.* Haettu 6.7.2021 osoitteesta <https://www.finlex.fi/fi/esitykset/he/2014/20140346.pdf>
- HE. (56/2017). *Hallituksen esitys eduskunnalle laeiksi aluevalvontalain ja rikoslain 17 luvun 7 b §:n muuttamisesta.* Haettu 16.11.2021 osoitteesta <https://finlex.fi/fi/esitykset/he/2017/20170056.pdf>
- HE. (198/2017). *Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.* Haettu 13.7.2021 osoitteesta <https://finlex.fi/fi/esitykset/he/2017/20170198.pdf>
- HE. (201/2017). *Hallituksen esitys eduskunnalle laeiksi rajavartiolain ja ulkomaalaislain muuttamisesta sekä eräksi niihin liittyviksi laeiksi.* Haettu 30.9.2021 osoitteesta <https://www.finlex.fi/fi/esitykset/he/2017/20170201.pdf>
- HE. (202/2017). *Hallituksen esitys eduskunnalle siviilitiedustelua koskevaiksi lainsäädännöksi.* Haettu 12.2.2021 osoitteesta <https://www.finlex.fi/fi/esitykset/he/2017/20170202.pdf>
- HE. (203/2017). *Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräksi siihen liittyviksi laeiksi.* Haettu 12.2.2021 osoitteesta <https://www.finlex.fi/fi/esitykset/he/2017/20170203.pdf>
- Heinonen, T. (2019). *Uusien tiedustelulakien valmistelu ja intressit (Pro gradu -tutkielma).* Itä-Suomen yliopisto. Haettu 13.7.2021 osoitteesta <https://erepo.uef.fi/handle/123456789/21557>
- Helenius, M. (2020). *"Tämä ei voi olla kansallisen kokonaisedun mukaista." – Suojelupoliisin tiedustelulakeihin liittyvät näkemykset ja perustelut eduskunnan valiokunnille vuoden 2018 valmistelutyön aikana (Pro gradu -tutkielma).* Helsingin yliopisto. Haettu 13.7.2021 osoitteesta <http://urn.fi/URN:NBN:fi:hulib-202004201864>
- Helin, S. & Rigatelli, S. (2021). *Trumpin potkiminen somesta oli PR-temppu, jolla on vaikutuksia sinunkin internetiisi – 6 asiaa jotka sinun pitää tietää.* Yle Uutiset 16.1.2021. Haettu 16.11.2021 osoitteesta <https://yle.fi/uutiset/3-11738815>
- Higgins, E. (2021). *Me olemme Bellingcat: Tiedustelupalvelu verkossa.* (A. Helasvuo, suom.) Jyväskylä: Docendo Oy.

- Hilbert, M. (2015). *Quantifying the Data Deluge and the Data Drought*. Taulukkopäivitykset varsinaiseen artikkeliin : Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332(6025), 60–65. Haettu 11.2.2021 osoitteesta <https://dx.doi.org/10.2139/ssrn.2984851>
- Hiltunen, L. (2009). Validiteetti ja reliabiliteetti. *Graduryhmä*, 18, 2009. Haettu 25.1.2022 osoitteesta http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf
- Hiltunen, A-K. (2021). *Valko-Venäjän painostus onnistuu, jos Eurooppa kiertää pakolaisoikeutta*. Kolumni julkaisussa *Ulkopolitiikka*, 3/2021. Haettu 2.11.2021 osoitteesta <https://ulkopolitiikka.fi/lehti/3-2021/anna-kaisa-hiltunen-valko-venajan-painostus-onnistuu-jos-eurooppa-kiertaa-pakolaisoikeutta/>
- Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita*. 21. painos. Porvoo: Bookwell Oy.
- Hoffman, F. (2009). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum, Number 240, April 2009*, s. 1–8. Haettu 21.12.2021 osoitteesta <https://apps.dtic.mil/dtic/tr/fulltext/u2/a496471.pdf>
- HS. (2017). *Rajavartiolaitos valmistautuu hybridiuhkien torjuntaan*. Pääkirjoitus, Helsingin Sanomat. 18.7.2017. Haettu 30.9.2021 osoitteesta <https://www.hs.fi/paakirjoitukset/art-2000005294381.html>
- Hyytiäinen, M. (2017). Hybridivaikuttaminen. Teoksessa J. Kielenniva, M. Hyytiäinen, H. Hovi, C. Fjäder, J. Raitasalo, K. Himberg, J. Eskola & J. Mölsä, *Turvallinen Suomi 2018 – Tietoja Suomen kokonaisturvallisuudesta*. Helsinki: Lönnberg Print & Promo.
- ITU. (2019). *Measuring Digital Development: Facts and Figures 2019*. Geneva: International Telecommunication Union. Haettu 11.2.2021 osoitteesta <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>
- Jansson, S. & Sihvonen, T. (2018). Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä* 41(1), 1–28. Haettu 6.1.2021 osoitteesta <https://doi.org/10.23983/mv.69950>
- Joentausta, J. (2022). *Mustajärvi: Tiedustelun toimivaltuuksia ei pidä laajentaa ennen kuin tiedustelulakien toimivuudesta on kattavampi kuva*. Kansan uutiset, uutinen, 9.2.2022. Haettu 9.2.2022 osoitteesta <https://urly.fi/2sRG>

- Jong, B., Duyvesteyn, I. & Reijn, J. (toim.). (2014). *The Future of Intelligence: Challenges in the 21st century*. New York: Routledge.
- Jowett, G. & O'Donnell, V. (2012). *Propaganda and Persuasion*. 5. painos. USA: SAGE Publications Inc.
- Juusti, J. (2021). *Kokonaisturvallisuutta yhdessä #1: Puheenjohtajan avajaistervehdys*. PLM kansliapäällikkö Jukka Juustin puhe. Haettu 17.3.2022 osoitteesta <https://turvallisuuskomitea.fi/kokonaisturvallisuutta-yhdessa-1-puheenjohtajan-avajaistervehdys/>
- Kaikkonen, A. (2021). *Puolustusministeri Antti Kaikkosen puhe Paasikivi-seurassa 19.1.2021*. Haettu 29.11.2021 osoitteesta <https://urly.fi/2kXM>
- Kivimäki, V-P. (2021). Esipuhe suomalaiselle lukijalle. Teoksessa E. Higgins, *Me olemme Bellingcat: Tiedustelupalvelu verkossa*. (A. Helasvuo, suom.) Jyväskylä: Docendo Oy.
- Kofman, M. (2021). *Zapad-2021: What to Expect From Russia's Strategic Military Exercise*. Artikkelijulkaisussa War on the Rocks. Haettu 9.11.2021 osoitteesta <https://warontherocks.com/2021/09/zapad-2021-what-to-expect-from-russias-strategic-military-exercise/>
- Kurttila, M. (2015). *MITÄ TIEDUSTELUSTA KIRJOITETTIIN? – Suojelupoliisi ja tiedonhankintalakyryryhmä mediassa 2013–2015* (Pro gradu -tutkielma). Tampereen yliopisto. Haettu 6.1.2021 osoitteesta <http://urn.fi/URN:NBN:fi:uta-201506291903>
- Laki esitutkintalain 2 luvun 1 §:n ja 9 luvun 6 §:n muuttamisesta. (585/2019).
- Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta. (584/2019).
- Laki poliisin hallinnosta annetun lain 10 ja 15 a §:n muuttamisesta. (583/2019).
- Laki poliisilain muuttamisesta (581/2019). Tutkielmassa käytetty ajantasaista lainsäädäntöä (poliisilaki 872/2011) ajan hetkeltä 1.1.2021. Haettu 1.1.2021 osoitteesta <https://www.finlex.fi/fi/laki/ajantasa/2011/20110872>
- Laki puolustusvoimista annetun lain muuttamisesta. (591/2019).
- Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa. (255/2014).
- Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain muuttamisesta. (592/2019).

- Laki sotilastiedustelusta. (590/2019). Tutkielmassa käytetty ajantasaista lainsäädäntöä ajan hetkeltä 1.1.2021. Haettu 1.1.2021 osoitteesta <https://finlex.fi/fi/laki/ajantasa/2019/20190590>
- Laki Suomen perustuslain 10 §:n muuttamisesta. (817/2018).
- Laki tietoliikennetiedustelusta siviilitiedustelussa. (582/2019). Tutkielmassa käytetty ajantasaista lainsäädäntöä ajan hetkeltä 1.1.2021. Haettu 1.1.2021 osoitteesta <https://www.finlex.fi/fi/laki/ajantasa/2019/20190582>
- Laki tuloverolain 92 b §:n muuttamisesta. (593/2019).
- Lankinen, T. (2018). *Valtioneuvoston selvitys- ja tutkimussuunnitelma 2019 – taustamuistio*. Valtioneuvoston kanslia. Haettu 29.11.2021 osoitteesta <https://valtioneuvosto.fi/delegate/file/45504>
- Lasconjarias, G. & Larsen, J. (toim.). (2015). *NATO's Response to Hybrid Threats*. Rome: NATO Defense College.
- Lehmus, L. (2010). *Venäjän lapsiasiamies kummeksuu Suomen huostaanottomääriä*. YLE ulkomaan uutiset, 19.3.2010. Haettu 2.11.2021 osoitteesta <https://yle.fi/uutiset/3-5530735>
- Leppänen, T. (2018). *Ministeriöiden ja yritysten näkemykset tietoliikennetiedustelusta : Tiedonhankintalakityöryhmän mietinnön lausuntokierros* (Pro gradu -tutkielma). Turun yliopisto. Haettu 13.7.2021 osoitteesta <https://www.utupub.fi/handle/10024/144739>
- Liang, Q. & Xiangsui, W. (1999). *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House. Haettu 30.11.2021 osoitteesta <https://www.cryptome.org/cuw.htm>
- Libicki, M. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.
- Limnell, J. (2021). Vaihtoehtoja selontekomenettelylle. Artikkelijulkaisussa *Kylkirauta*. N:o 292, 3/2021. ss. 13–17.
- Limnell, J. & Iloniemi, J. (2018). *Uhkakuvat*. Jyväskylä: Docendo Oy.
- Lonka, H., Laitinen, K., Keinänen, A., Wähä, S., Huhtinen, A-M. & Paasonen, J. (2020). *Kansallisen turvallisuuden vaikutusten arviointi*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2020:28. Haettu 6.1.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-287-950-9>

- Luotonen, A. (2022). *Näin Venäjä pyrkii hajottamaan, hämmentämään ja hallitsemaan – mihin Suomen on syytä varautua?* Yle Uutiset, 3.2.2022. Haettu 9.2.2022 osoitteesta <https://yle.fi/uutiset/3-12298888>
- LVM. (2015). *Itämeren kansainvälinen ilmatila turvallisemmaksi yhteistyöllä*. Liikenne- ja viestintäministeriön tiedote 13.1.2015. Haettu 9.11.2021 osoitteesta <https://www.lvm.fi/-/itameren-kansainvalinen-ilmatila-turvallisemmaksi-yhteistyolla-796331>
- Mannonen, L. (2020). *"Miksi emme luottaisi?" retorinen tarkastelu suomalaisen tiedustelulainsäädännön lähetekeskustelusta* (Pro gradu -tutkielma). Jyväskylän yliopisto. Haettu 6.1.2021 osoitteesta <http://urn.fi/URN:NBN:fi:ju-202005263474>
- Martin, K. (2004). Domestic Intelligence and Civil Liberties. *The SAIS Review of International Affairs*, 24(1), 7–21. Haettu 21.12.2021 osoitteesta <https://www.jstor.org/stable/26999197>
- Mikkola, H., Aaltola, M., Wigell, M., Juntunen, T. & Vihma, A. (2018). *Hybridivaikuttaminen ja demokratian resilienssi: Ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa*. FIIA raportti 55. Haettu 28.10.2021 osoitteesta <https://www.fia.fi/julkaisu/hybridivaikuttaminen-ja-demokratian-resilienssi>
- Moore, C. (2019). *Russia and Disinformation: The Case of Ukraine*. Tutkimusraportti, julkaisija The Centre for Research and Evidence on Security Threats (CREST). Haettu 8.11.2021 osoitteesta <https://crestresearch.ac.uk/download/2407/19-022-01.pdf>
- Myers, M. (2019). *Qualitative Research in Business and Management*. 3. painos. London: SAGE Publications Ltd.
- Mykkänen, J. & Virtanen, J. (2020). Hallituksen muodostaminen: Katosiko strateginen hallitusohjelma? Teoksessa S. Borg, E. Kestilä-Kekkonen & H. Wass (toim.), *Politiikan ilmastonmuutos: Eduskuntavaalitutkimus 2019*. Oikeusministeriön julkaisuja 2020:5. Haettu 11.5.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-259-838-7>
- National Post. (2017). *NATO performs large-scale drill in Suwalki Gap – where Russia could make its first move if war broke out*. Uutinen 19.7.2017, World news, National Post. Haettu 9.11.2021 osoitteesta <https://urly.fi/2iNC>
- Nevaste, N. (toim.). (2016). *Katsaus hybridituhkiin ja niiden vaikutuksiin*. Turvallisuuskomitean kevätkokouksen 2016, seminaarijulkaisu. Haettu 26.2.2021 osoitteesta <https://turvallisuuskomitea.fi/katsaus-hybridituhkiin-ja-niiden-vaikutuksiin/>

- Niemonen, R. (2021). *Ylen kysely: Sosiaalinen media vaikuttaa lähes joka toisen äänestyspäätökseen kuntavaaleissa – tulos yllätti tutkijankin*. Yle Uutiset, 30.1.2021. Haettu 9.2.2022 osoitteesta <https://yle.fi/uutiset/3-11761178>
- Niinistö, S. (2018). Tasavallan presidentti Sauli Niinistön puhe 227. maanpuolustuskurssin avajaisissa 5.11.2018. Haettu 1.2.2021 osoitteesta <https://www.presidentti.fi/puheet/>
- Nilsen, T. (2017). *Norway well prepared to meet Russian jamming*. Artikkelijulkaisussa The Barents Observer. Haettu 9.11.2021 osoitteesta <https://thebarentsobserver.com/en/node/3327>
- Nordström, H., Laitinen, K., Lundelin, M., Herrala, J., Sjöblom, J., Honkanen, K. & Nurminen, M. (2015). *Suomalaisen tiedustelulainsäädännön suuntaviivoja: Tiedonhankintalakiyöryhmän mietintö*. Puolustusministeriö, 14.1.2015. Haettu 2.3.2021 osoitteesta https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf
- Nordström, H., Honkanen, K., Melaluoto, J., Pellikainen, T., Nurminen, M., Vira-Klockars, T. & Kari, M. (2017). *Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Työryhmän mietintö*. Puolustusministeriö, 19.4.2017. Helsinki: Lönnberg Print & Promo. Haettu 7.6.2021 osoitteesta <http://urn.fi/URN:ISBN:978-951-25-2899-8>
- Nykter, N. (2018). *Knowing Me, Knowing You - National Cyber Security Situation Understanding Within a Network of Actors* (Pro gradu -tutkielma). Maanpuolustuskorkeakoulu. Haettu 2.2.2021 osoitteesta <http://urn.fi/URN:NBN:fi-fe2018080233296>
- Ohra-aho, H. (2019). Puolustusvoimien tiedustelupäällikkö, kenraalimajuri. *Suomen sotilastiedustelu* (Radio Kipinä podcast -haastattelu). Kausi 2, jakso 11. Haettu 22.1.2021 osoitteesta <https://puolustusvoimat.fi/asiointi/kanavat/radio-kipina/podcastit> sekä tekstimuotoinen tiivistelmä osoitteesta <https://ruotuvaki.fi/-/tiedustelupaallikko-ohra-aho-sotilastiedustelun-lahteet-ja-suorituskyky-pidettava-salassa>
- Omand, D. & Phythian, M. (2018). *Principled Spying: The Ethics of Secret Intelligence*. Washington DC: Georgetown University Press.
- Pelttari, A. (2021). Twitter-kommentti 19.12.2021. Haettu 27.1.2022 osoitteesta <https://twitter.com/pelttariantti/status/1472578396186202116>

- Pekola, S. (2018). *Tiedustelu oikeusvaltiossa: tiedustelutoimivaltuuksien laajentaminen tiedustelun valvonnan näkökulmasta* (Pro gradu -tutkielma). Lapin yliopisto. Haettu 6.1.2021 osoitteesta <http://urn.fi/URN:NBN:fi:ula-201809131328>
- Perry, T. (2018). Move over, Moore's law. Make way for Huang's law [Spectral Lines]. *IEEE Spectrum* 55(5), 7-7. Haettu 22.9.2021 osoitteesta <https://doi.org/10.1109/MSPEC.2018.8352557>
- Pietiläinen, T. (2021). *Supo haluaa lisää oikeuksia tiedustella salaa – laillisuusvalvojat täsmentäisivät nykyisiä tiedustelulakeja*. HS Poliitiikan uutiset, 23.11.2021. Haettu 29.11.2021 osoitteesta <https://www.hs.fi/politiikka/art-2000008422934.html>
- Pietiläinen, T. (2022). *Tiedustelulakien toimivuus sai kiitosta eduskunnassa – ei valmiutta antaa lisää salaisia tiedonhankintakeinoja Supolle*. HS Poliitiikan uutiset, 9.2.2022. Haettu 9.2.2022 osoitteesta <https://www.hs.fi/politiikka/art-2000008587572.html>
- Pitkänen, S. & Sutinen, V-J. (2018). *Propagandan historia – kuinka meihin on vaikuttettu antiikista infosotaan*. Helsinki: Into Kustannus.
- Pulkkinen, E. (2017). *Suomeen kaavailtu epätyypillisen sodankäynnin keskus kiinnostaa – "Tärkeä rooli Nato-yhteistyössä"*. Esa Pulkkinen haastattelu MTV Uutisiin, 11.2.2017. Haettu 29.11.2021 osoitteesta <https://urly.fi/2kXQ>
- Puolustusministeriö. (2013). *Kansallisen lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyöyn parantamiseksi kybertoimintaympäristön uhkista; lainsäädäntöhanke*. Asettamispäätös 13.12.2013. Haettu 8.7.2021 osoitteesta https://www.defmin.fi/files/2669/Kyberlainsaadantotyoryhman_asettamispaatos.pdf
- Puolustusministeriö. (2015). *Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintakityöryhmän mietintö*. 14.1.2015. Haettu 12.7.2021 osoitteesta https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf
- Puolustusministeriö. (2019). *Hallituksen esitys HE 203/2018 vp laiksi sotilastiedustelusta ja eräksi siihen liittyviksi laeiksi: Kysymyksiä ja vastauksia*. Haettu 12.7.2021 osoitteesta https://www.defmin.fi/files/4543/Q_A_sotilastiedustelu110319.pdf
- Puolustusvoimat. (2021a). *Sotilastiedustelu: Julkinen katsaus 2021*. Pääesikunta. Haettu 6.5.2021 osoitteesta

https://puolustusvoimat.fi/documents/1948673/74055459/PV_sotilastiedustelu_raportti_www_FI_2021.pdf

Puolustusvoimat. (2021b). Pääesikunnan tiedusteluosasto. Haettu 22.6.2021 osoitteesta <https://puolustusvoimat.fi/tietoa-meista/paaesikunta/tiedusteluosasto>

PuVM. (9/2018). *Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi*. Puolustusvaliokunnan mietintö 1.3.2019. Haettu 19.7.2021 osoitteesta https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/PuVM_9+2018.pdf

Pynnöniemi, K. & Saari, S. (2017). Hybrid influence – lessons from Finland. Artikkelijulkaisussa *NATO Review*, 28.6.2017. Haettu 28.10.2021 osoitteesta <https://urly.fi/2hl9>

Pöysti, T. (2021). *Tiedustelulainsäädäntöä koskeva valtioneuvoston selonteko*. Lausunto 19.3.2021. OKV/565/21/2021. Haettu 29.8.2021 osoitteesta <https://www.okv.fi/fi/lausunnot/id/163/>

Rantala, J. (2021). Suojelupoliisin esikuntapäällikön twiitti 19.12.2021, haettu 11.1.2021 osoitteesta <https://twitter.com/JyriRantala/status/1472578644707008522>

Rifkin, J. (2011). *The Third Industrial Revolution: How Lateral Power is Transforming Energy, The Economy, and The World*. New York: Palgrave Macmillan

Rodriguez, C., Walton, T., & Chu, H. (2020). Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power. *Joint Force Quarterly* 97(2), 121–128. Haettu 10.11.2021 osoitteesta <https://apps.dtic.mil/sti/pdfs/AD1099537.pdf>

Rumbim, S. (2020). *Sisäisen turvallisuuden uhkakuvat ja muutos Sisäministeriön hallinnonalan asiakirjoissa 2004–2017* (Pro gradu -tutkielma). Helsingin yliopisto. Haettu 19.9.2021 osoitteesta <http://urn.fi/URN:NBN:fi:hulib-202009023998>

Ruotuväki. (2017). *Rajavartiolain uudistus vastaa hybridiuhkiin*. Artikkelijulkaisu, 14.9.2017. Haettu 30.9.2021 osoitteesta <https://ruotuvaki.fi/-/rajavartiolain-uudistus-vastaa-hybridiuhkiin>

Sandell, M. (2021). *Näin Suomi selviää tulevista kriiseistä: huippututkijat ehdottavat tehokkaita ilmastotekoja, medialukutaidon vahvistamista ja panostusta henkiseen hyvinvointiin*. Yle Uutiset, 8.2.2021. Haettu 9.2.2022 osoitteesta <https://yle.fi/uutiset/3-11772468>

- Sebastian, K. (2019). Distinguishing Between the Types of Grounded Theory: Classical, Interpretive and Constructivist. *Journal for Social Thought* 3(1), 1–9. Haettu 10.5.2022 osoitteesta <https://ojs.lib.uwo.ca/index.php/jst/article/view/4116>
- Siljoranta, S. (2020). *Avointen lähteiden tiedustelun tarkastelu tiedustelulakien näkökulmasta* (Pro gradu -tutkielma). Jyväskylän yliopisto. Haettu 22.2.2021 osoitteesta <http://urn.fi/URN:NBN:fi:jyu-202012157153>
- Sinderbrand, R. (2017). *How Kellyanne Conway ushered in the era of 'alternative facts'*. Trumpin kampanjapäällikkö ja neuvonantaja Kellyanne Conwayn haastattelu ja litterointi. Haettu 19.2.2021 osoitteesta <https://www.washingtonpost.com/news/the-fix/wp/2017/01/22/how-kellyanne-conway-ushered-in-the-era-of-alternative-facts/>
- Singer, P. & Brooking, E. (2018). *LikeWar: The Weaponization of Social Media*. New York: HMH Books.
- Sisäministeriö. (2004). *Arjen turvaa – Sisäisen turvallisuuden ohjelma*. Valtioneuvoston yleisistunto 23.9.2004. Sisäasiainministeriön julkaisuja 44/2004.
- Sisäministeriö. (2014). *Suojelupoliisin hallinnollista asemaa ja tulosoajasta sekä valvonnan kehittämistä seloittaneen työryhmän loppuraportti*. Sisäministeriön julkaisu 28/2014. Haettu 9.7.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-491-993-7>
- Sisäministeriö. (2016). *Valtioneuvoston selonteko sisäisestä turvallisuudesta*. Sisäministeriön julkaisu 8/2016. Haettu 1.2.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-324-085-8>
- Sisäministeriö. (2017). *Siviilitiedustelulainsäädäntö. Työryhmän mietintö*. Sisäministeriö, julkaisu 8/2017, 19.4.2017. Haettu 8.6.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-324-129-9>
- Sisäministeriö. (2017b). *Parlamentaarinen seurantaryhmä tiedustelulainsäädännön valmistelulle ja perustuslain tarkistamiselle*. Tiedote 5.5.2017. Haettu 13.7.2021 osoitteesta <https://intermin.fi/-/parlamentaarinen-seurantaryhmatiedustelulainsaadannon-valmistelulle-ja-perustuslain-tarkistamiselle>
- Sisäministeriö. (2017c). *Tiedustelulaki kirvoitti laajasti lausuntoja, palaute pääosin myönteistä*. Sisäministeriön tiedote 075/2017, 11.7.2017. Haettu 19.7.2021 osoitteesta <https://valtioneuvosto.fi/-/1410869/tiedustelulaki-kirvoitti-laajasti-lausuntoja-palaute-paaosin-myonteista>

- Sisäministeriö. (2019a). *Kansallinen riskiarvio 2018*. Sisäministeriön julkaisuja 2019:5. Haettu 25.5.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-324-245-6>
- Sisäministeriö. (2019b). *Siviilitiedustelulain esittely*. Näyttöesitys 11.3.2019, Sisäministeriö. Haettu 22.1.2021 osoitteesta <https://intermin.fi/tiedustelu>
- Sisäministeriö. (2019c). *Siviilitiedustelulainsäädäntöä täydennetään kahdella asetuksella*. Sisäministeriön tiedote 41/2019. Haettu 7.9.2021 osoitteesta <https://intermin.fi/-/siviilitiedustelulainsaadantoa-taydennetaan-kahdella-asetuksella>
- Sisäministeriö. (2019d). *Rajavartiolaitoksen valtuuksia puuttua hybridiuhkiin lisätään*. Sisäministeriön tiedote 1/2019. Haettu 30.9.2021 osoitteesta <https://intermin.fi/-/rajavartiolaitoksen-valtuuksia-puuttua-hybridiuhkiin-lisataan>
- Silvonen, J. & Keso, P. (1999). Grounded theory aineistolähtöisen analyysin mallina. *Psykologia : tiedepoliittinen aikakauslehti*, 34(2), 88–96.
- Smith, H. (2019). Countering hybrid threats. Teoksessa G. Lindstrom & T. Tardy (toim.), *NATO and the EU: The essential partners*, 15–24. NATO Defense College. Haettu 11.1.2022 osoitteesta <http://www.jstor.org/stable/resrep19964.7>
- Suojelupoliisi. (2017). *Suojelupoliisin vuosikirja 2016*. Julkaistu 29.3.2017. Haettu 6.7.2021 osoitteesta https://supo.fi/documents/38197657/40760236/2016_Supo_vuosikirja.pdf
- Suojelupoliisi. (2020). *Kansallisen turvallisuuuden katsaus 2020*. Julkaistu 29.10.2020. Haettu 22.1.2021 osoitteesta https://supo.fi/documents/38197657/39761269/FI+Kansallisen+turvallisuuuden+katsaus_2020.pdf
- Suojelupoliisi. (2021a). *Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi*. Suojelupoliisin tiedote 18.3.2021. Haettu 17.3.2022 osoitteesta <https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi>
- Suojelupoliisi. (2021b). *Suojelupoliisin vuosikirja 2020*. Julkaistu 23.3.2021. Haettu 6.7.2021 osoitteesta <https://urly.fi/26lu>
- Tanner, R. (2019). *SUOMEN KYBERTURVALLISUUSSTRATEGIA JA TIEDUSTELULAKIUUDISTUS : Turvallisuuongelmia vai turvallistamisiongelmiä?*

(Pro gradu -tutkielma). Tampereen yliopisto. Haettu 6.1.2021 osoitteesta <http://urn.fi/URN:NBN:fi:tuni-201904021458>

Tiilikainen, T. (2020). *Teija Tiilikainen: Hybridivaikuttaminen on kylmäävään laajaa*. Haastattelu T. Tiilikainen, tekstin kirjoittanut Leeni Peltonen. Haettu 29.9.2021 osoitteesta <https://www.erillisverkot.fi/teija-tiilikainen-hybridivaikuttaminen-on-kylmaavan-laajaa/>

Tikka, I. (2021). *USA:ssa vallanvaihto lähestyy – Ääriliiketutkija Ylelle: "Viranomaisien täytyy varautua väkivaltaan koko maassa, ei pelkästään Washingtonissa"*. Yle Uutiset, 16.1.2021. Haettu 9.2.2022 osoitteesta <https://yle.fi/uutiset/3-11740151>

Toivonen, T. (2021). *Opposition mielestä Suomi on varautunut huonosti siirtolaisten käyttämiseen painostuskeinona – jättivät yhteisen välikysymyksen hybridiuhkista*. YLE politiikan uutiset, 16.11.2021. Haettu 16.11.2021 osoitteesta <https://yle.fi/uutiset/3-12189700>

Torstila, P. (2020). *Open Skies ja Suomi – Etykin asevalvontaneuvottelut 1990–1992*. Artikkelijulkaisussa *Sotilasaikakauslehti*. N:o 993, 5/2020. ss. 70–75.

Turvallisuuskomitea. (2014). *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma*. 11.3.2014. Haettu 12.7.2021 osoitteesta <https://urly.fi/26TL>

Ulkoministeriö. (2010). *Suomen ulko- ja turvallisuuspoliittisesta päätöksentekojärjestelmästä*. 3.3.2010. Haettu 1.2.2021 osoitteesta https://um.fi/documents/35732/48132/suomen_ulko__ja_turvallisuuspoliittisesta_paatoksente_kojarjestelmasta/

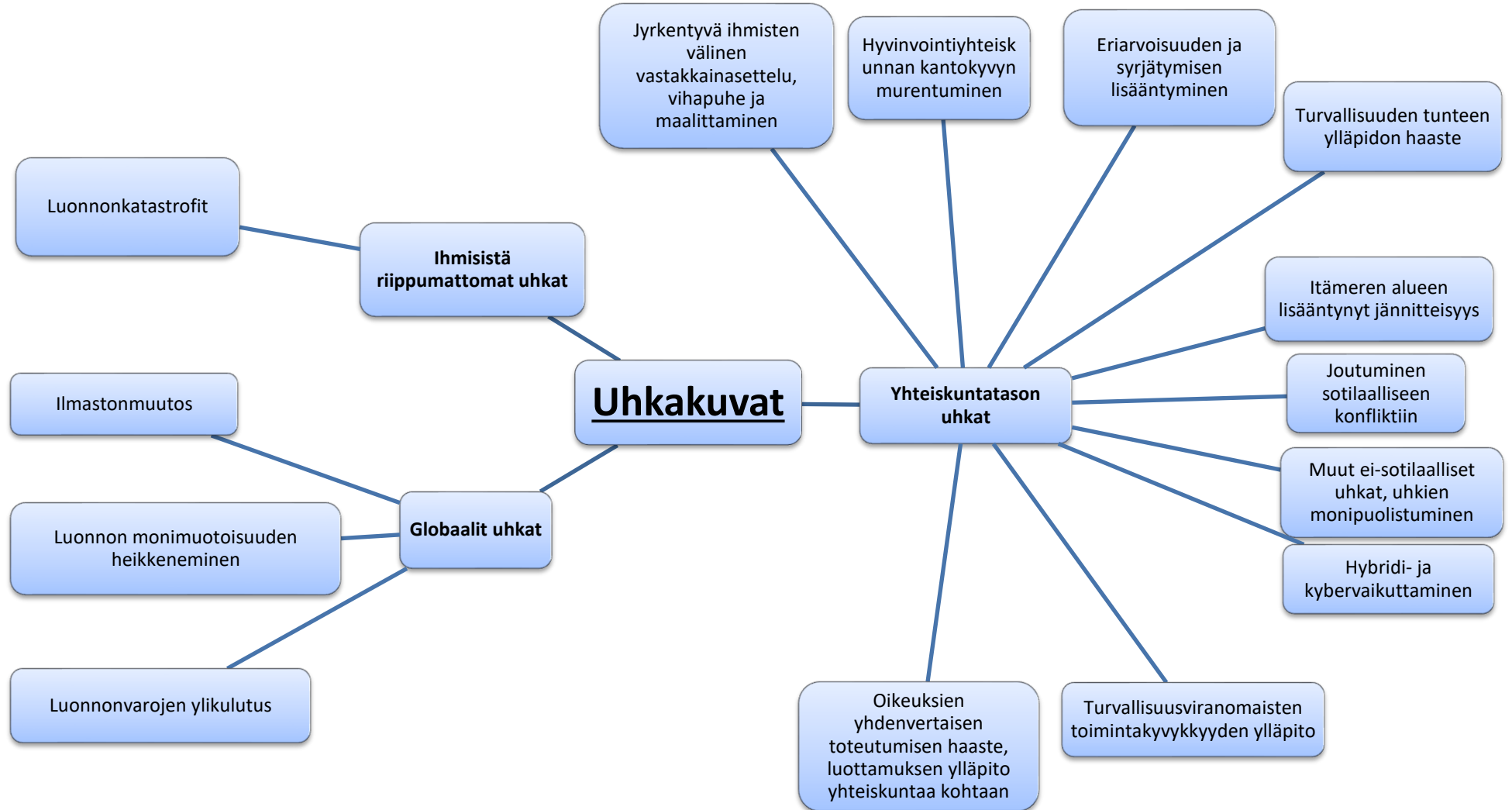
Valtioneuvosto. (2013). *Suomen kyberturvallisuusstrategia*. Valtioneuvoston periaatepäätös 24.1.2013. Haettu 8.7.2021 osoitteesta <https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf>

Valtioneuvosto. (2017). *Valtioneuvoston puolustusselonteko*. Valtioneuvoston kanslian julkaisusarja 5/2017. Haettu 22.2.2021 osoitteesta https://www.defmin.fi/files/3683/J05_2017_VN_puolustusselonteko_Su_PLM.pdf

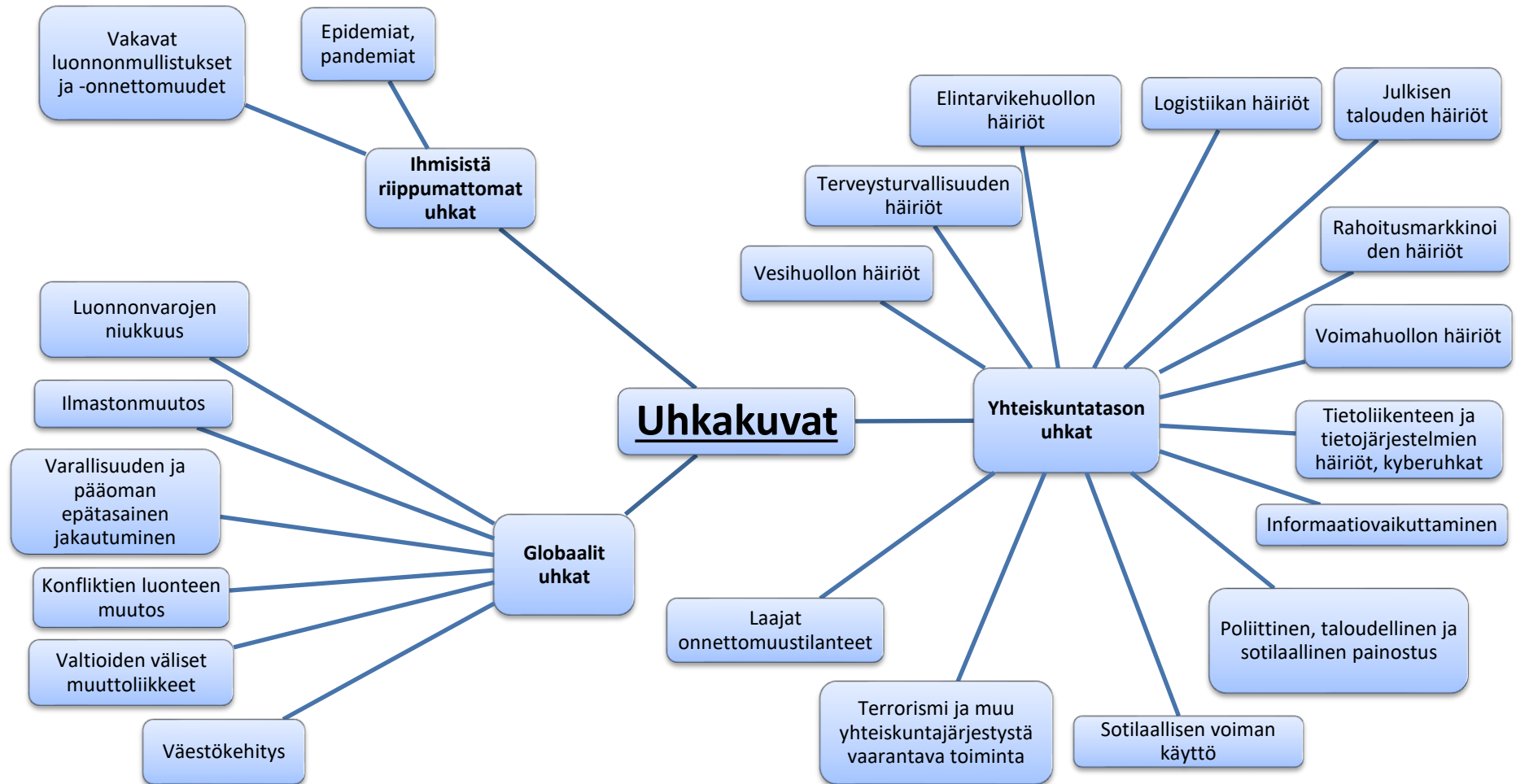
Valtioneuvosto. (2019). *Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019*. Valtioneuvoston julkaisuja 2019:31. Haettu 22.2.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-287-808-3>

- Valtioneuvosto. (2020). *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko*. Valtioneuvoston julkaisuja 2020:30. Haettu 1.2.2021 osoitteesta <http://urn.fi/URN:ISBN:978-952-287-876-2>
- Valtioneuvosto. (2021). Periaatepäätökset. Haettu 25.5.2021 osoitteesta <https://valtioneuvosto.fi/paatokset/periaatepaatokset>
- Waldrop, M. (2016). The chips are down for Moore's law. *Nature*, vol. 530, 144–147. Haettu 1.2.2021 osoitteesta <https://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338>
- Wikforss, Å. (2020). *Vaihtoehtoiset faktat*. (P. Tuomisto, suom.) Helsinki: Kustannusosakeyhtiö Aula & Co.
- Wright, D. & Kreissl, R. (2014). *Surveillance in Europe*. London: Routledge.
- YTS. (2017). *Yhteiskunnan turvallisuusstrategia*. Valtioneuvoston periaatepäätös 2.11.2017. Haettu 18.2.2021 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

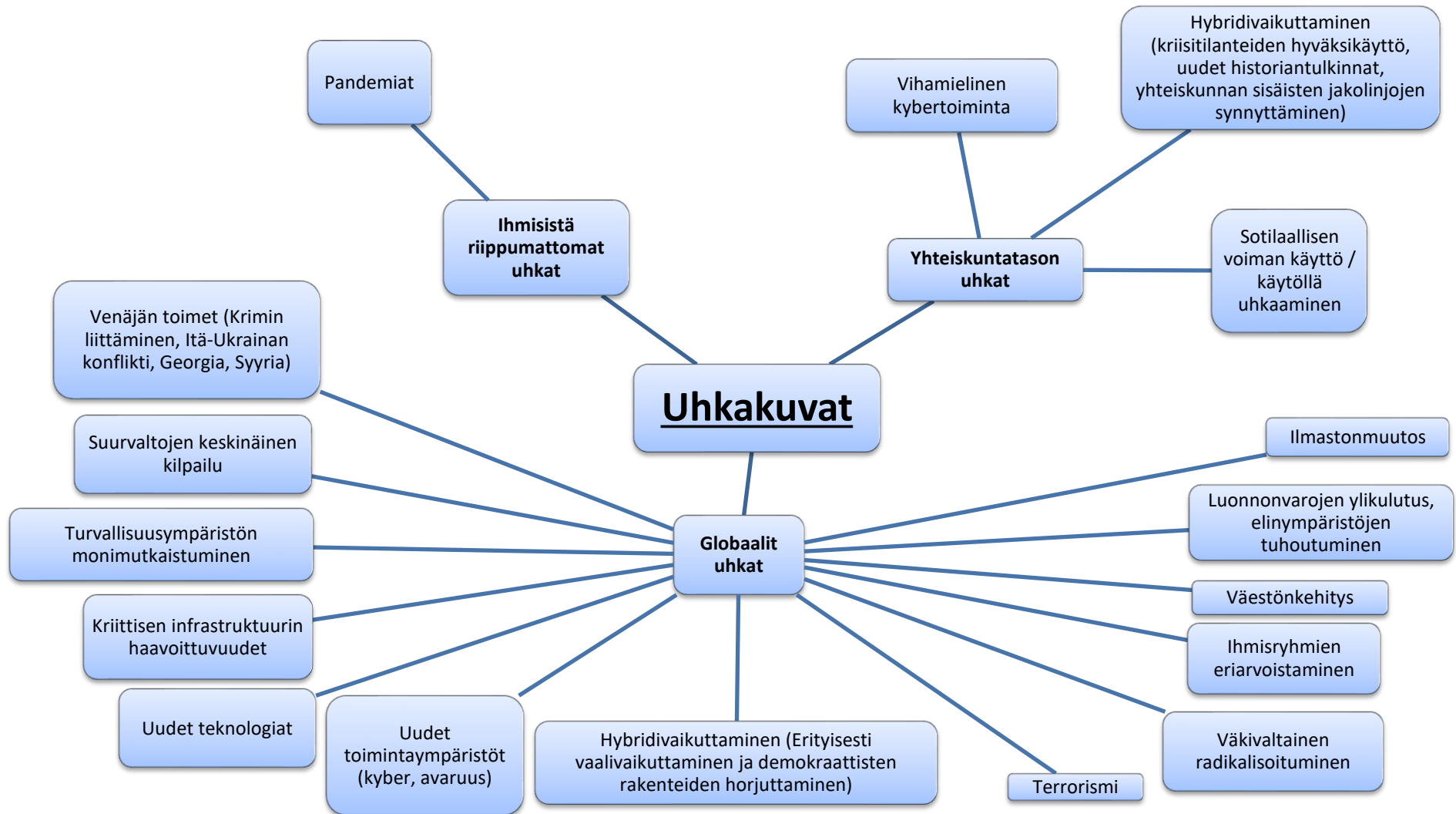
LIITE 1 KANSALLINEN UHKAKUVAKÄSITE HALLITUSOHJELMAN MUKAISESTI



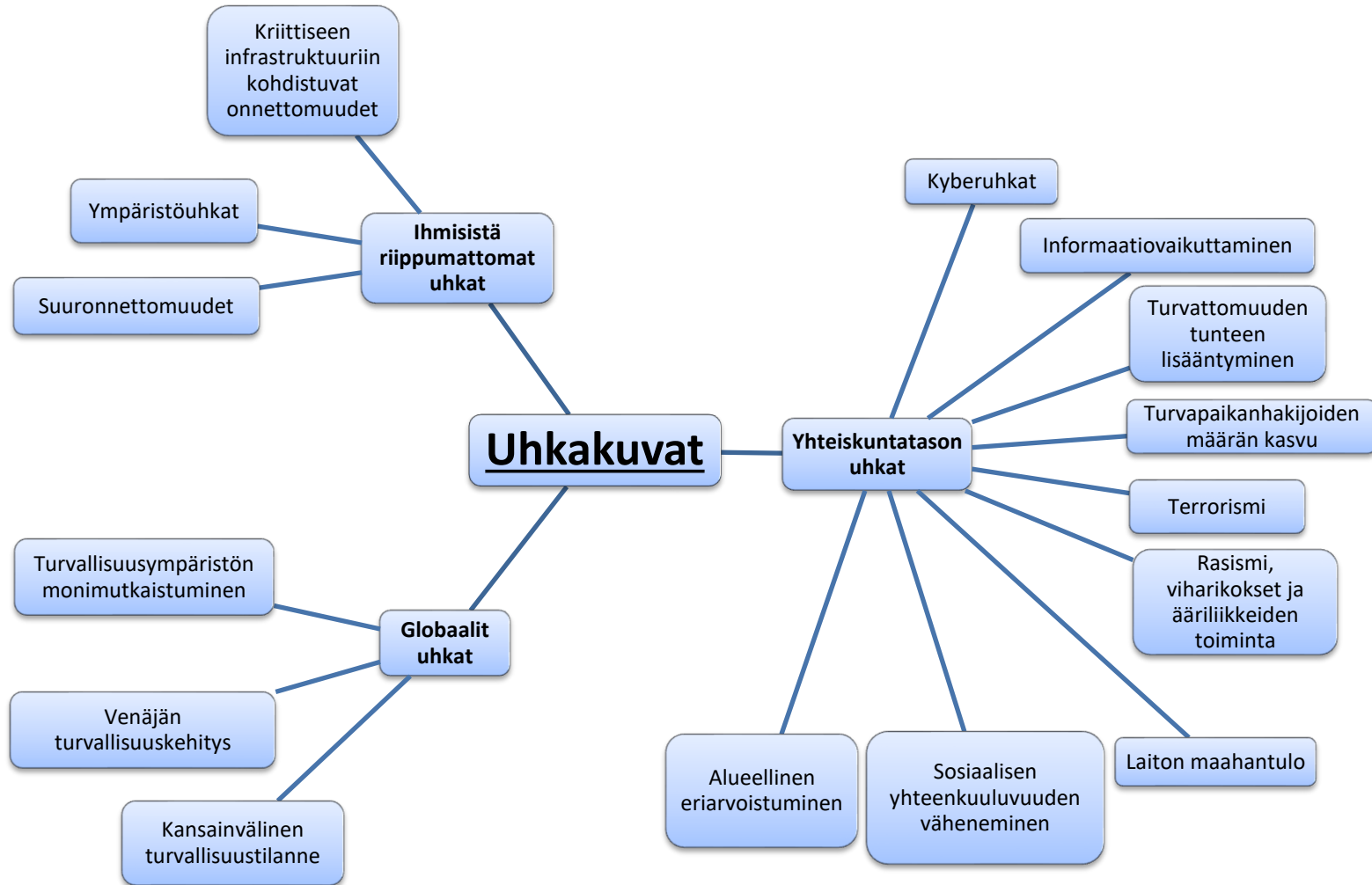
LIITE 2 KANSALLINEN UHKAKUVAKÄSITE KANSALLISEN RISKIARVION MUKAISESTI



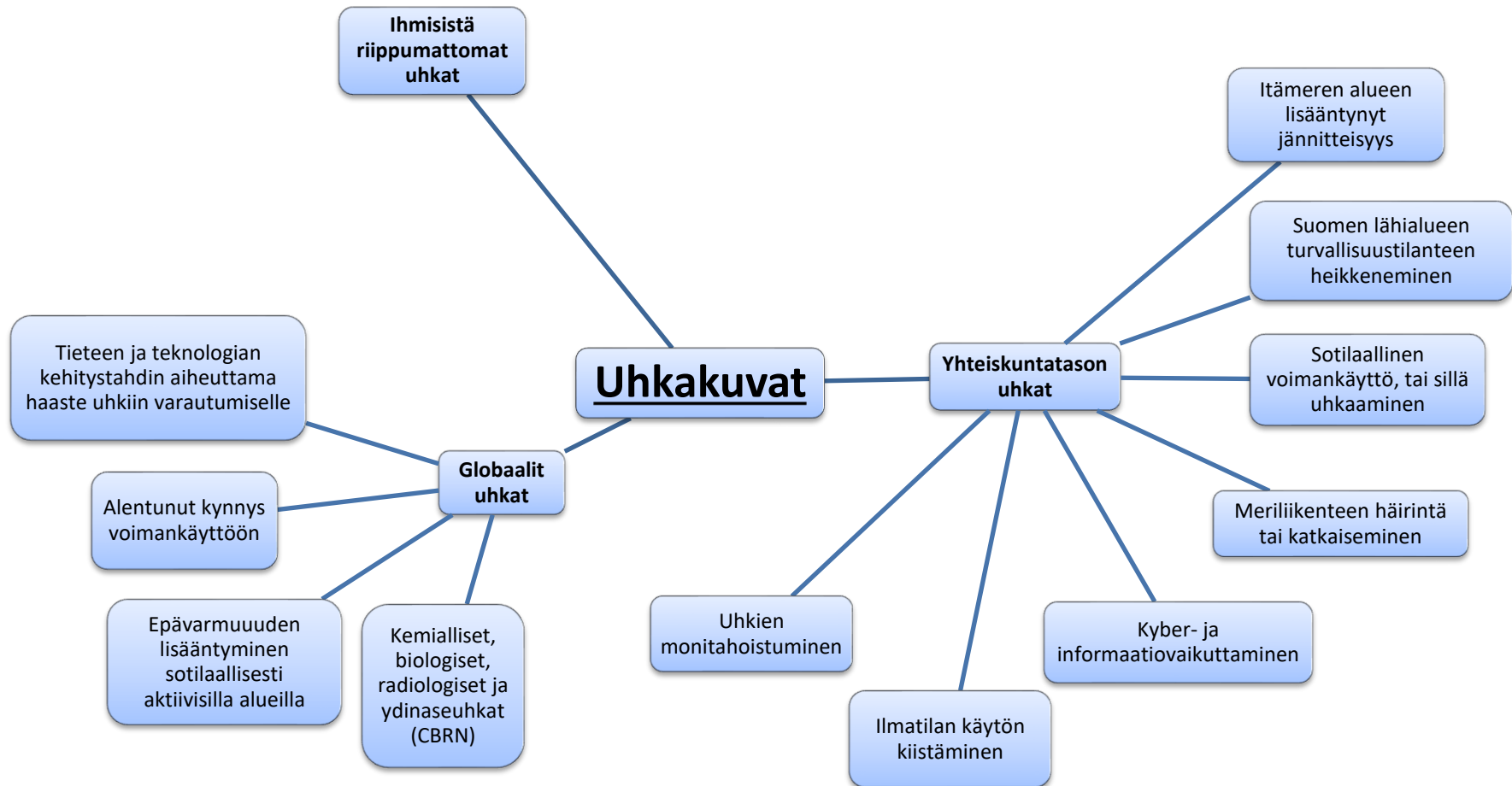
LIITE 3 KANSALLINEN UHKAKUVAKÄSITE ULKO- JA TURVALLISUUSPOLIITTISEN SELONTEON MUKAISESTI



LIITE 4 KANSALLINEN UHKAKUVAKÄSITE SISÄISEN TURVALLISUUDEN SELONTEON MUKAISESTI



LIITE 5 KANSALLINEN UHKAKUVAKÄSITE PUOLUSTUSSELONTEON MUKAISESTI



LIITE 6 TURVALLISUUSASIAKIRJOJEN MUODOSTAMA KANSALLINEN UHKAKUVAKÄSITE

